OFFICECONNECT™ REMOTE

510, 520, 530

USER GUIDE

Please read the Supplementary Information section of this manual for details of the OfficeConnect 531 model and an EMC Update

Part No. 980/000033/001
Published January 1996

3Com Corporation ■ 5400 Bayfront Plaza ■ Santa Clara, California ■ 95052-8154

© 3Com Sonix Limited, 1996. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without permission from 3Com Sonix. 3Com Sonix reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Sonix to provide notification of such revision or change. 3Com Sonix provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com Sonix may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:
If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following restricted rights:

For units of the Department of Defense: *Restricted Rights Legend:* Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) for restricted Rights in Technical Data and Computer Software clause at 48 C.F.R. 52.227-7013. 3Com Sonix Limited, Merchants' House, Wilkinson Road, Cirencester, Gloucestershire, GL7 1YT.

For civilian agencies: *Restricted Rights Legend:* Use, reproduction or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software - Restricted Rights Clause at 48 C.F.R. 52.227-19 and the limitations set forth in 3Com Corporation's standard commercial agreement for the software. Unpublished rights reserved under the copyright laws of the United States.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT. If you are unable to locate a copy, please contact 3Com Sonix and a copy will be provided to you.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, Boundary Routing and Transcend are registered trademarks of 3Com Corporation. OfficeConnect is a trademark of 3Com Corporation. 3Com Laser Library, 3TECH, CacheCard and SmartAgent are trademarks of 3Com Corporation. 3ComFacts and are service marks of 3Com Corporation.

CompuServe is a registered trademark of CompuServe, Inc. Castelle is a registered trademark of Castelle Corporation. Novell and NetWare are registered trademarks of Novell Inc. Windows is a trademark of Microsoft Corporation. VT100 is a registered trademark of Digital Equipment Corporation.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

IMPORTANT SAFETY INFORMATION

WARNING: *Warnings contain directions that you must follow for your personal safety. Follow all instructions carefully.*

Please read carefully and thoroughly the following information before installing the OfficeConnect Remote:

- Exceptional care must be taken during installation and removal of the unit.
- Only stack the OfficeConnect Remote with other OfficeConnect units.
- Only use the power adapter that is supplied with the unit to ensure compliance with international safety standards.
- It is essential that the mains socket outlet is located near the unit and is accessible. You can only remove power to the OfficeConnect Remote by disconnecting the power adapter from the unit or from the socket outlet.
- The safety status of the interconnection port on this equipment are as follows:

  Ports identified by the labels VOICE and ISDN = TNV

  Ports identified by the labels SERIAL, COAX, 10BASET and WAN = SELV

  TNV (telecoms network voltage) is a circuit which under normal operating conditions carries telecommunication signals.

  SELV (safety extra low voltage) is a secondary circuit which is designed and protected so that under normal and single-fault conditions, the voltage between any two accessible parts does not exceed a safe value (42.2 V peak or 60 V DC).

  Only connect apparatus complying with the relevant interface requirements to the ports on this unit..
- There are no user-replaceable fuses or user-serviceable parts inside the unit. If you have a physical problem with the unit that cannot be solved with problem solving actions in this guide, contact your supplier.
- Disconnect the power adapter before moving the unit.

WARNING: Twisted Pair RJ45 data port. *This is a shielded RJ45 data socket. It cannot be used as a telephone socket. Only connect RJ45 data connectors to this socket.*

WICHTIGE SICHERHEITSHINWEISE

ACHTUNG: *Die Warnungen enthalten Anweisungen, die Sie zur eigenen Sicherheit zu befolgen haben.*

Lesen Sie bitte die folgenden Informationen sorgfältig durch, bevor Sie den OfficeConnect Remote einbauen:

- Auf besondere Vorsicht muß während des Ein- und Ausbaus des OfficeConnect Remotes geachtet werden.
- Stapeln Sie den OfficeConnect Remote nur mit anderen OfficeConnect Einheiten zusammen.
- Verwenden Sie nur das mit dem OfficeConnect Remote mitgelieferte Netzteil um die internationalen Sicherheitsstandards zu erfüllen.
- Die Netzsteckdose muß sich in unmittelbarer Nähe des OfficeConnect Remotes befinden und frei zugänglich sein. Sie können den OfficeConnect Remote nur spannungsfrei schalten, indem Sie das Steckernetzteil aus der Netzsteckdose ziehen oder die Verbindung zum Gerät unterbrechen.
- Der Sicherheitsstandard der Anschlüsse fuer dieses Gerät sind wie folgt:

  Anschlüsse bezeichnet mit VOICE und ISDN = TNV

  Anschlüsse bezeichnet mit SERIAL, COAX, 10BASET und WAN = SELV

  TNV (Telecoms Network Voltage - Spannung des Telekommunikationsnetzwerks) ist ein Anschluss, der unter normalen Umständen Telekommunikationssignale enthält .

  SELV (Safety Extra Low Voltage - Extra Sicherheitsspannung) ist ein weiterer Anschluss, der unter normalen Umständen und Fehlerkonditionen entworfen und gesichert wurde, so dass die Spannung zwischen zwei erreichbaren Teilen kein gefährliches Niveau erreicht (42.2V max. oder 60 V DC).

  An den Anschlussbuchsen der Geräte dürfen nur die dafür vorgesehenen Anschlüsse verwendet werden.

- Es sind keine von dem Benutzer zu ersetzende oder zu wartende Teile in dem Gerät vorhanden. Wenn Sie ein Problem mit dem OfficeConnect Remote haben, das nicht mittels der Fehleranalyse in dieser Anleitung behoben werden kann, setzen Sie sich mit Ihrem Lieferanten in Verbindung.
- Bevor der OfficeConnect Remote ausgebaut wird ist das Netzteil zu ziehen.

ACHTUNG: gedrehte paarfache RJ45 Datenanschluss. *Es ist eine abgeschirmte RJ45 Datenanschlußbuchse. Sie darf nicht als Telefonanschluß verwendet werden. Verbinden Sie nur RJ45 Datenstecker mit diesem Anschluss.*

L'INFORMATION DE SÉCURITÉ IMPORTANTE

AVERTISSEMENT: *Les avertissements contiennent les instructions que vous devez suivre pour votre sécurité personnelle. Suivre toutes les instructions avec soin.*

Veuillez lire à fond l'information suivante avant d'installer le moyeu:

- Le soin exceptionnel doit être pris pendant l'installation et l'enlèvement du moyeu.
- Seulement entasser le moyeu avec les autres moyeux OfficeConnects.
- Seulement utiliser la pièce de raccordement d'alimentation qui est fournie avec le moyeu pour assurer la conformité avec les normes de sécurité internationales.
- C'est essentiel que le socle de prise de courant du réseau soit localisé proche du moyeu et soit accessible. Vous pouvez seulement enlever l'alimentation au moyeu en débranchant la pièce de raccordement d'alimentation de l'unité ou du socle de prise de courant.
- Les normes de sécurité des ports d'interconnexion sur cet équipement sont les suivants:

  Les ports marqués par les etiquettes VOICE et ISDN = TNV

  Les ports marqués par les etiquettes SERIAL, COAX, 10BASET et WAN = SELV

  TNV (Telecoms Network Voltage - tension réseau de télécommunications) est un circuit qui dans des conditions d'opérations normales, transfert les signeaux télécoms.

  SELV (Safety Extra Low Voltage - tension de sécurité extra-réduite) est un circuit secondaire désigné et protègé qui dans des conditions normales et de fautes uniques, assure que la tension entre deux éléments accessibles n'accedéra pas un niveau de sécurité (42.2V max. ou 60 V DC).

  Connecter uniquement des unités conformes aux normes relatives des interfaces de cet équipement.

- Il n'y a pas de parties remplaceables par les utilisateurs ou entretenues par les utilisateurs à l'intérieur du moyeu. Si vous avez un problème physique avec le moyeu qui ne peut pas être résolu avec les actions de la résolution des problèmes dans ce guide, contacter votre fournisseur.
- Débrancher la pièce de raccordement d'alimentation avant de remuer le moyeu.

AVERTISSEMENT: Le port de données RJ45 de paire tordue. *Ceux-ci est un socle de données RJ45 blindé. Il ne peut pas être utilisé comme socle de téléphone. Seulement brancher les connecteurs de données RJ45 à ce socle.*

CONTENTS

IMPORTANT SAFETY INFORMATION
WICHTIGE SICHERHEITSHINWEISE
L'INFORMATION DE SÉCURITÉ IMPORTANTE

ABOUT THIS GUIDE

Introduction 1
How to Use This Guide 1
Conventions 2
Additional Safety Information 3

1 GETTING STARTED

Introduction 1-1
- OfficeConnect Remote Features 1-1
- Benefits of ISDN 1-3
- Pack Contents Checklist 1-4
- Registering Ownership Of Your OfficeConnect Remote 1-5
- Pre-installation Requirements 1-5
- OfficeConnect Remote Front and Rear Panel Features 1-6

Installation 1-10
- Siting the OfficeConnect Remote 1-10

Using the Rubber Feet and Stacking Clips 1-11
- Wall Mounting the OfficeConnect Remote 1-12
- Connecting the Power Adapter 1-12
- Connecting to Your 10BaseT LAN 1-13
- Connecting to a Single Workstation 1-14
- Connecting to Your 10Base2 LAN 1-14
- Connecting to ISDN 1-15
- Connecting to the WAN 1-16
- Connecting to the VOICE Port 1-16
- Connecting a Management Terminal 1-16
- Location of OfficeConnect Fax and Print Servers 1-16

Quick Configuration 1-17
- Starting Quick Configuration 1-17
- About Quick Configuration 1-19
- Setting the Unit Name 1-20
- Connecting to a Novell (IPX) Network 1-21
- Connecting to an IP Host on the Same IP Network 1-22
- Connecting to an IP Host on a Different IP Network 1-23
- Connecting to the Internet or a PPP Router 1-25

Monitoring ISDN Line Usage 1-28
Setting Up a WAN Link 1-28
Examples of Typical ISDN Networking Applications 1-30
Novell Network 1-30
IP Host on the Same IP Network 1-31
IP Host on Another IP Network 1-33
Internet or PPP Router 1-34
Multiple Connections from a Single Site 1-35
Troubleshooting 1-36

A BRIDGING AND ROUTING

Introduction A-1
Bridging and Routing Concepts A-1
Guidelines For Choosing Bridging or Routing A-2
How Bridges Learn A-2
Bridging Between Remote Sites A-3
Building a Larger Network A-4
Multiple Paths Between Bridged LANs A-5
Network Topology A-6
Broadcast Storms A-6
Optimum Use of Resource A-6
Network Organization, Structure and Physical Layout A-7
The Internet A-7
Routing IP and IPX A-7
IP Routing A-9
IPX Routing A-11
IP Addresses A-12
Numbered and Unnumbered Links A-15

B TECHNICAL INFORMATION

Specifications B-1
LAN Connector Interfaces B-1
WAN Connector Interface B-1
ISDN Connector Interface B-1
Voice Connector Interface B-1
Management Connector Interface B-1
Bridge Characteristics B-2
Performance B-2
Approvals B-2
FCC Requirement B-3
Dimensions B-4
Interface Cable Characteristics B-5
WAN Port Connecting Cable – V.11/X.21 Support B-5
WAN Port Connecting Cable – V.24/V.28 Support B-6
WAN Port Connecting Cable – V.35/V.36 Support B-7
Manager Port Connecting Cable B-8
Modem Cable B-9
LAN Port Connecting Cable - 10BaseT B-9
Ordering Information B-10

C GLOSSARY

D TECHNICAL SUPPORT

On-line Technical Services D-1
3Com Bulletin Board Service D-1
World Wide Web Site D-2
Support from Your Network Supplier D-2
Support from 3Com D-2
Returning Products for Repair D-3

INDEX

ABOUT THIS GUIDE

Introduction

This guide describes the features, installation and initial configuration of the OfficeConnect Remote. The guide has been designed to be used by both first-time and experienced computer network users who want to install and use the OfficeConnect Remote. xxx

If you are working with an ISDN bridge or router for the first time, it is possible you may make mistakes. We have tried to identify the likely errors you may make and have provided hints and tips to help you recover from error situations.

Once you have carried out the intial configuration of the unit using the *Quick Configuration* option you can carry out additional configuration to optimize the unit's performance on your network. Refer to the *Software Reference* guide for more details.

How to Use This Guide

This table shows where to find specific information:

If you are looking for information on:	Turn to:
About the OfficeConnect Remote's features, a description of the front panel indicators and rear panel connectors and step-by-step installation and configuration instructions.	Chapter 1
An overview of bridging and routing and an introduction to IP and IPX protocols.	Appendix A
Technical Information and cable specifications	Appendix B
Glossary of technical terms	Appendix C
Technical Support information	Appendix D

Conventions

The icon conventions that are used throughout this guide are:

Icon	Type	Description
	Information Note	Information notes call attention to important features or instructions.
	Caution	Cautions alert you to personal safety risk, system damage, or loss of data.
	Warning	Warnings alert you to the risk of severe personal injury.

The text conventions used in this guide are:

Convention	Description
"Enter" vs. "Type"	When the word "enter" is used in this guide, it means type something, then press the [Return] or [Enter] key. Do not press the [Return] or [Enter] key when an instruction simply says "type."
Text represented as `screen display`	`This typeface` is used to represent displays on your screen, for example: `Enter the unit's IP address:`
Text represented as **`commands`**	**`This typeface`** is used to represent commands that you enter, for example: **`CO IS NU`**
Keys	When specific keys are referred to in the text, they are called out by their labels, such as "the Return key" or "the Escape key," or they may be shown as [Return] or [Esc]. If two or more keys are to be pressed simultaneously, the keys are linked with a plus sign (+), for example: Press [Ctrl]+[Alt]+[Del].
Italics	*Italics* are used to denote *new terms* or *emphasis*.

Additional Safety Information

See also the Important Safety Information at the front of this guide.

- When using the unit, observe the following safety information:
- Retain this user's guide for later use and pass it on in the event of change of ownership of the unit.
- The power adapter supplied with the unit is fitted with a moulded plug, for connection to a standard electrical mains system supply socket. If this plug is not suitable for your connection to your mains supply, contact your reseller for advice. On no account should you attempt to connect to your mains supply using an inappropriate mains adapter.
- Protect the unit from sudden, transient increases and decreases in electrical power by fitting an in-line surge suppresser or uninteruptable power supply.
- Products manufactured by us are safe and without risk provided they are installed, used and maintained in good working order in accordance with our instructions and recommendations.
- If any of the following conditions occur, isolate the electricity supply and refer to your 3Com reseller.
  - If the case or cover is not correctly fitted.
  - If the case is damaged.
  - If the unit begins to make an odd noise, smell or smoke.
  - If the unit shows signs of a distinct change in performance.
- Never install telephone wires during a lightening storm, or install telephone connection sockets in wet locations, unless the socket is specifically designed for wet locations.
- Do not touch uninstalled telephone wires or terminals unless the telephone line has been disconnected at the network interface. Always exercise caution when installing or modifying telephone lines.
- Do not use a telephone, which is connected to the unit, to report a gas leak in the vicinity of the leak.
- Do not spill food or liquids on the unit. If the unit gets wet, isolate the electrical supply and contact your 3Com reseller.

- Do not push any objects into the openings of the unit. Doing so can cause fire or electric shock by shorting out internal components.
- Avoid using a telephone, which is connected to the unit (other than a cordless type), during an electrical storm. There may be a remote risk of electric shock from lightning.
- Equipment connected to the Voice port must be located in the same building as the unit.
- Be sure nothing rests on the unit's system cables and that the cables are not located where they can be stepped on and cause damage to the unit.
- Keep the unit away from radiators and heat sources. Allow 25mm (1 inch) around the unit to provide adequate air circulation.
- Install the unit in a clean area that is free from dust or extreme temperatures.
- The unit has been designed to be a free standing unit or stacked with other OfficeConnect units. Do not place anything else on top of the unit's case.
- Allow a clearance gap of at least a 150 mm from the rear panel of the unit, to allow for cable access.
- This product ostensibly complies with the electro-magnetic compatibility (EMC) requirements of EN 55022 Class A and EN 50082 (susceptibility). However, to fully comply with Class B of EN55022 the following prerequisites should be observed;
  - the WAN port must be attached to a screened digital cable.
  - the ISDN cable must be used in conjunction with a three turn ferrite.
- This unit contains a lithium battery which is attached to a microchip on the printed circuit board. The defective battery must be disposed of safely in-line with the manufacturers instructions.
- Interconnecting directly, or by way of other apparatus, to ports complying with SELV requirements may produce hazardous conditions on the network. Advice should be sought from a competent engineer before such a connection is made.

1 GETTING STARTED

Introduction

Welcome to the world of inter-networking with 3Com®. This chapter contains all the information you need to install and configure the OfficeConnect Remote to make it operational. You can carry out more sophisticated configuration using the information in the *Software Reference* guide.

In the modern business environment sharing information is crucial. Until now only large businesses could afford the high speed connections between offices to gain the networking advantage. The OfficeConnect Remote changes this and provides high speed, low cost inter-networking for small offices and home users.

The OfficeConnect Remote is ideal for linking together remote offices or workgroups. It is compact and attractively designed for desktop use and is part of the OfficeConnect™ range which neatly stack together with clips to provide a host of other facilities, for example, Ethernet hub, print sharing and network fax.

OfficeConnect Remote Features

The OfficeConnect Remote is designed to connect a LAN (Local Area Network) at one location with a number of other LANs at remote locations. The LAN could comprise any number of PCs, servers or other computing equipment, which in an office or small business environment are typically linked together using a centrally located OfficeConnect hub. In order to interconnect the hubs in different locations, the OfficeConnect Remote unit transmits information over a WAN (Wide Area Network) service provided by telephone carrier organizations.

The most modern and efficient of these WAN services includes ISDN (Integrated Services Digital Network). This provides a high speed dialup facility to allow your OfficeConnect Remote to automatically and quickly dial remote offices, transmit your data between remote PCs just as speedily and then disconnect the call. You incur minimum ISDN telephone charges as calls are made only when needed. This is known as Dial on Demand.

ISDN can also be used to make voice calls using the OfficeConnect Remote from an ordinary telephone handset, connect faxes and other similar office equipment. All OfficeConnect Remote models have facilities for ISDN data transmission. Some models have an additional port for voice calls and/or a port to handle a third category of connection over a serial WAN port.

The WAN port connects to a permanent leased line, also available from your telephone carrier organization. Leased lines are available to work at a range of speeds which incur higher costs the higher the line speed. The benefit of leased lines is their permanence and fixed cost. No dialling is required but unlike ISDN you pay a fixed cost regardless of whether you transfer little data or high volumes of data 24 hours a day.

Overall ISDN is probably the most cost effective solution for small businesses. However, if your requirements to move data between sites is likely to increase you should consider purchasing the OfficeConnect Remote model fitted with both ISDN and WAN ports to ensure increased flexibility. The range of OfficeConnect Remote units is as follows:

- **OfficeConnect Remote 510** – Provides connection from 10BaseT or Thin Ethernet (10Base2) LANs to ISDN services for data transfer between remote sites.
- **OfficeConnect Remote 520** – In addition to the data transfer facilities, this model has a Voice port allowing a telephone (or other equipment such as a Fax) to communicate via ISDN.
- **OfficeConnect Remote 530** – This model has the ISDN and Voice port facilities and additionally the ability to connect via a WAN port to a serial leased line.

  All of the above models are available with *U* or *S* ISDN interfaces.

  Typically, the OfficeConnect Remote is used to interconnect LANs running protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP) or Novell Internetwork Packet Exchange (IPX). Offering full LAN-to-LAN connectivity at speeds up to 64 Kilobits per second (Kbps) on each ISDN channel and up to2 Megabits per second (Mbps) on the WAN port (where fitted), the OfficeConnect Remote is a compact desktop unit with unrivalled price and performance.

The principal features of the OfficeConnect Remote are:

- Easy to install, configure and support.
- ISDN, 2B+D port, supporting Basic Rate interface of two 64 Kbps (or two 56 Kbps channels in the USA) and a 16 Kbps control channel.
- Optional voice port.
- Optional Leased line wide area network (WAN) access port.
- Data terminal equipment (DTE) management port
- Support for full IP and IPX routing.
- Protocol transparent bridging.
- Sophisticated data packet filtering to provide network security.
- Provides NetWare protocol *spoofing*.
- Data compression based on an optimized Lempel Ziv algorithm.
- Remote and local management.
- Flash erasable programmable read-only memory (EPROM), allowing the remote upgrading of the units operating system.
- Uses simple network management protocol (SNMP) and provides management information base (MIB) II support.

Benefits of ISDN

ISDN is an extension of the national and international public switched telephone network, which offers a digital end-to-end telecommunication system, providing a better quality service than available using the analog telephone network. The principal benefits of ISDN are:

- Fast call setup times, typically taking less than one second for national calls.
- Greater bandwidth with multiple channels.

  The basic rate service, often referred to as ISDN 2, carries two 64 Kbps user channels, called B channels and one 16 Kbps control channel called the D channel. The line service is presented into the customers premises through a standard RJ45 socket.

  A significant aspect of the ISDN service is that it can be provided over the same wiring that was installed for the original telephone service. Therefore, ISDN can be made available relatively cheaply almost anywhere that previously had access to the analog system.

  The cost of installation and rental of basic rate ISDN lines has dropped to the point where it is extremely attractive as regards cost and performance.

Using ISDN to Support Leased Line WAN Circuits

ISDN provides an ideal service to connect remote LANs. To be effective, the connecting bandwidth needed is at least 64 Kbps to achieve a realistic throughput. Slower speed links can be used but usually only when usage is low and infrequent, or if higher speed circuits cannot be provided.

Leased digital point-to-point circuits can still be cost effective if usage spans many hours per day. However as ISDN tariffs reduce, this balance also changes. ISDN can be used to provide effective backup of these point-to-point WAN circuits in two ways.

- Firstly, if the point-to-point circuit fails, an ISDN channel can be dialled-up automatically and quickly, to provide an alternative path to the remote unit.
- Secondly, if the leased circuit becomes heavily loaded due to peaks in the traffic between remote bridges or routers, additional bandwidth can be automatically dialled-up to supplement the bandwidth of the leased circuit. The interconnected bridges would then treat the leased line and ISDN channel as parallel links, sharing the load across the two.

Pack Contents Checklist

Before you install your OfficeConnect Remote, check the contents of the box against the pack contents checklist below. If any of the items have been damaged in transit or are missing, then contact the 3Com dealer from whom the equipment was purchased.

- 1 x OfficeConnect Remote unit.
- 1 x power adapter fitted with an appropriate plug for your national power supply.
- 1 x 1.5 meter RJ45 to RJ45 male plug ISDN 2 connecting cable.
- 1 x 1.5 meter DB9 to DB9 serial manager port cable.
- 1 x British Telecom to RJ11 convertor (UK models of OfficeConnect Remote 520 and 530 only).
- 1 x OfficeConnect Remote *User Guide*.
- 1 x OfficeConnect Remote *Software Reference* guide.
- 1 x Warranty Registration Card.

It is important that you save the unit's box and protective packing material in case you need to store, or transport it in the future.

Registering Ownership Of Your OfficeConnect Remote

A warranty registration card is enclosed in the box with your OfficeConnect Remote. Please take a few moments before commencing the installation to fill in the card and post it to us.

Pre-installation Requirements

Before you install your OfficeConnect Remote you will need the following:

- A suitable cable for connection to your LAN (or workstation if only a single workstation is attached to this unit).

Although the OfficeConnect Remote has two LAN connections (10Base2 and 10BaseT), only one port can be used at a time.

- A standard ISDN line wall socket to connect the ISDN cable to the ISDN port of the OfficeConnect Remote. If a suitably sited wall socket is not already available, then contact your telecommunications supplier for assistance.
- A suitable cable to connect to your ISDN socket. A 1.5 meter ISDN cable is supplied with this unit.
- The ISDN telephone number of the remote ISDN unit in order to carry out the connection configuration procedure.
- A suitable WAN cable if you are connecting to the remote site over a leased line.

OfficeConnect Remote Front and Rear Panel Features

Front Panel

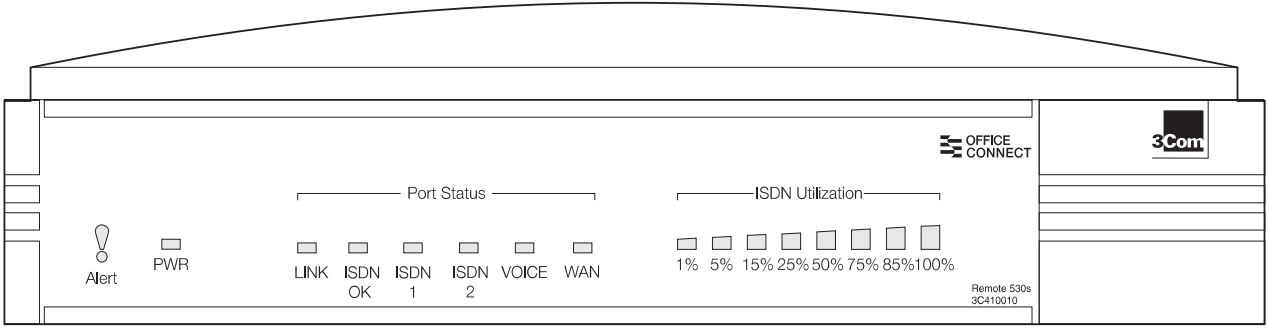


Figure 1-1 OfficeConnect Remote Front Panel Features

! ALERT (Orange) This LED indicator shows four states.

- Off – Normal operation and no faults detected.
- Slow flash – Loading software during power up or new software is being downloaded to the unit.
- Quick flash – Self test during power up.
- On – Problem detected. Refer to "Troubleshooting" on page 1-38 for more information.

POWER (Green) This LED indicator shows three states:

- On – Power is connected to the unit.
- Slow flash – New software is being downloaded to the unit.

- Quick flash – Self test or software loading during power up.
- Off – No power supplied to the unit. See "Troubleshooting" on page 1-38 for more details.

LINK (Orange) This LED indicator shows the condition of the LAN connection:

- Off – No LAN connection detected.
- On – LAN connected.

ISDN OK (Green) This LED indicator provides confirmation of the state of the ISDN line.

- On – Indicates the OfficeConnect Remote is connected to a working ISDN line. Sometimes this LED does not light until the first call attempt is made.
- Flashing – A fault condition has been identified on the ISDN line.
- Off – No ISDN connection present.

ISDN1 and **ISDN 2** (Yellow) These LED indicators provide confirmation that an ISDN call is in progress on ISDN Channel 1 or Channel 2. You are connected to a remote ISDN unit and are incurring ISDN call charges while this LED is lit. If the LED is flashing it indicates that a call is being made but a connection has not yet been made to the remote unit.

VOICE (Yellow) If a Voice port is fitted this LED shows the status of the voice connection:

- On – A voice call is in progress.
- Flashing – Indicates that handset is off the hook and a dial tone is present or a call is being dialled or ringing out. It also shows if the handset is ringing (receiving an incoming call).

WAN (Yellow) This LED indicator provides confirmation of the state of the WAN link (if fitted). If the LED is lit, the WAN connection is valid and can pass data across the link. If the LED is flashing it indicates a fault on the WAN port.

ISDN Utilization (Green/Yellow) These LEDs show the ISDN utilization as a percentage of network loading. If you consistently see a continuous ISDN loading of 100% and you require faster throughput, then you might consider the following:

- You could configure the unit to filter some of the data. See the *Software Reference* guide for more information.
- An additional ISDN or WAN link is possibly required to cope with the amount of data you need to transfer.

Rear Panel

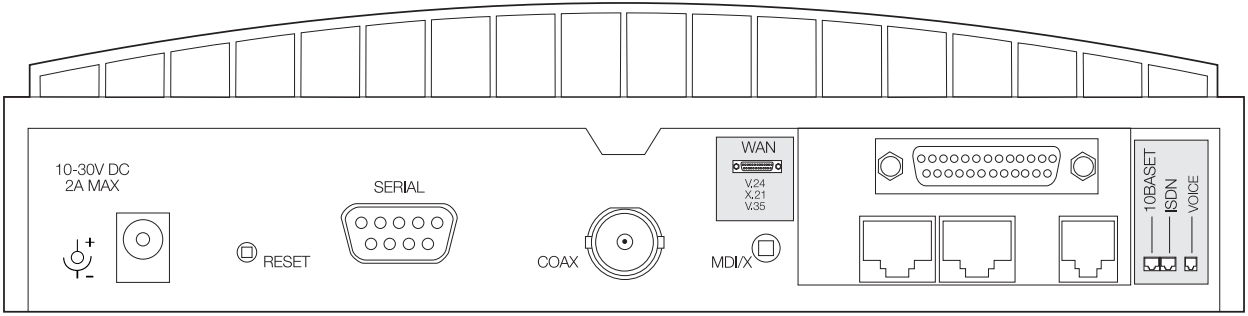


Figure 1-2 OfficeConnect Remote Rear Panel Features

POWER Only use the power adapter supplied with the OfficeConnect Remote to connect to the mains power supply. Do not use any other adapter with this unit. If the plug on the power adapter does not match the mains inlet socket, contact your reseller for further advice.

RESET For Technical Support use only.

SERIAL The Serial Manager port enables a management PC or terminal to be connected to the OfficeConnect Remote using the 9-pin V.24 Serial Manager cable supplied with the unit. The port provides VT100 terminal emulation, running at 9600 bps. Refer to Appendix B for more information about cables.

You also need a proprietary communications software package such as Windows 'Terminal' to communicate with the OfficeConnect Remote.

COAX (10Base2 Coaxial Port) – The coaxial LAN port allows a 10Base2 Ethernet segment to be connected directly to the OfficeConnect Remote. If the unit is to be installed at the end of a cable run, then a 50 Ohm terminator must be fitted to the 10Base2 cable connector. This port can be used to connect to OfficeConnect hubs.

MDI/MDIX Switch Affects the operation of the 10BaseT LAN port. If you are connecting to a hub, leave the switch in the *In* position. If you are connecting to a single PC, set the switch to the *Out* position to implement the 10BaseT crossover that is required.

WAN (OfficeConnect Remote 520 and 530 only) This port is used to provide connection to a WAN, via a private leased line. The port terminates with a 25-way D-type female connector. This port supports any of the CCITT data transmission standards; X.21/V.11 V.24/V.28 (RS232), and V.35/V.36 at data transfer rates up to 2 Mbps. Provided that connection cables that follow these standards are used, the OfficeConnect Remote automatically detects the type of interface that the port is required to support, and configure it accordingly.

Refer to Appendix B for information about the WAN interface cables required. Suitable cables are available from your 3Com reseller as spare parts, refer to Appendix B for required item part number

10BASET This RJ45 port is to the left of the ISDN socket when looking at the rear of the unit and is used to provide a connection to a 10BaseT LAN. This socket allows direct connection between the OfficeConnect Remote and a single piece of equipment, as opposed to multi-point LAN connections using 10Base2 cabling systems. The OfficeConnect Remote LAN port simulates the characteristics of a workstation port, which allows it to be directly connected to a LAN or network hub port as required.

If the LAN port is to be connected directly to a single PC or workstation, then you must implement the crossover by setting the MDI/MDIX switch to the out position. See “MDI/MDIX Switch” for more information.

ISDN This port is used to connect to the ISDN network. The port uses an RJ45 connection socket situated to the left of the 10BaseT LAN socket. A standard ISDN line wall socket is required to connect the ISDN cable to the ISDN port of the OfficeConnect Remote.

VOICE (where fitted) This port is used to connect an optional public switched telephone network (PSTN) telephone handset, or any other compatible analog equipment, operating in digital tone multiple frequency (DTMF) mode, by connecting the handset's plug into this port.

This port is in effect an analog to digital convertor which allows you to use your conventional PSTN telephone on an ISDN line. It is capable of supporting ringing current and call progress tones, and supports analog devices to a maximum ringer equivalence number (REN) of two (United Kingdom). Providing one of the two 64 Kbps ISDN channels is not being used by the unit, then a voice call can be made.

Incoming ISDN traffic carries both a voice and data identifier and depending on the type of transmission, a voice call is automatically directed to the appropriate port connected to the telephone handset.

The VOICE port is terminated with an RJ11 socket. If your telephone equipment uses a different connector jack, you will need to obtain a suitable convertor to connect to the VOICE port. A British Telecom to RJ11 convertor is supplied with UK models fitted with a Voice port.

Installation

Siting the OfficeConnect Remote

When siting the OfficeConnect Remote, ensure:

- It is accessible and cables can be easily connected.
- It is out of direct sunlight and away from sources of heat.
- Cabling is away from:
  - Sources of electrical noise, such as radios, transmitters and broadband amplifiers.
  - Power lines and fluorescent lighting fixtures.
- Water or moisture cannot enter the case of the unit.
- Air flow around the unit and through the vents in the side of the case is not restricted. We recommend that you provide a minimum of 25mm (approx. 1 inch) clearance around the unit.

To prolong the operational life of your equipment:

- Never stack OfficeConnect units more than four high and ensure that they are clipped securely together.
- Do not place objects on top of any unit or stack.

Using the Rubber Feet and Stacking Clips

The four self-adhesive rubber feet prevent your hub from sliding around on your desk. Stick the feet to the marked areas at each corner of the underside of your hub.

The four stacking clips are used for neatly and securely stacking your OfficeConnect units together. **You can stack up to a maximum of four units. Large units must be stacked below small units.** To stack your units, secure the clips on one side and then on the other. Use the following method to secure one side:

1. Place your new unit on a flat surface. Your clips fit in the positions on the side of the unit, as shown in Figure 1-3 (1).
2. Position a clip over one of these holes and push it in until it clicks into place, as shown in Figure 1-3 (2). Repeat this for the other clip position on the same side.
3. Keeping the front of the units aligned, rest the bottom of the new unit on the clips' spikes, as shown in Figure 1-3 (3). Push the clips firmly into the new unit until they click into place.

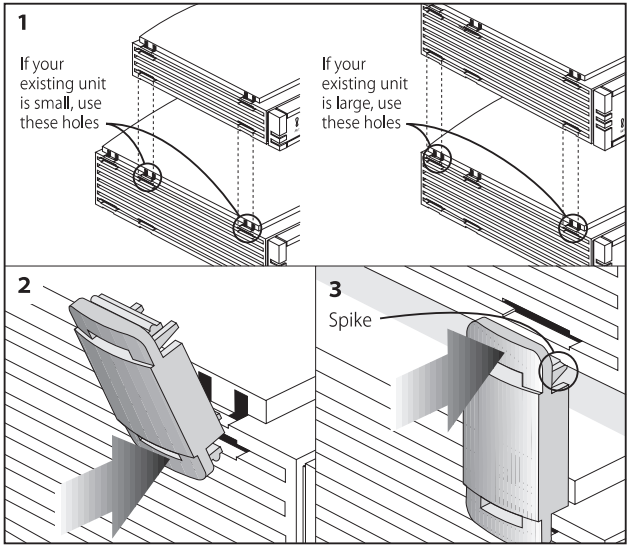


Figure 1-3 Clipping Your Units Together

Repeat these steps to secure the other side.

To remove a clip, hold the units firmly with one hand and hook the first finger of your other hand around the back of the clip. Use reasonable force to pull it off.

Wall Mounting the OfficeConnect Remote

There are two slots on the underside of the OfficeConnect Remote which are used for wall mounting. You can mount the unit with the LEDs facing upwards or downwards, to suit your needs.

When wall mounting your OfficeConnect Remote, ensure that it is within reach of the mains socket.

You need two suitable screws. Ensure that the wall you are going to use is smooth, flat, dry and sturdy. Make two screw holes which are 142 mm (5.6 in) apart. Fix the screws into the wall, leaving their heads 3 mm (0.12 in) clear of the wall surface.

Remove any connections to the units and locate it over the screw heads. When in line, gently push the OfficeConnect Remote on to the wall and move it downwards to secure. When making connections, be careful not to push the unit up and off the wall.

CAUTION: *Only wall mount single units, do not wall mount stacked units.*

Connecting the Power Adapter

CAUTION: *First, read the section; "Important Safety Information" at the start of this manual.*

Isolate the electrical mains system supply before commencing installation.

Ensure any on/off power switches at the outlet socket are set to their 'OFF' positions.

1 Connect the jack of the power adapter to the socket on the rear panel of the OfficeConnect Remote (see "Rear Panel" on page 1-8).

2 Plug the mains lead of the power adapter into an adjacent electrical mains system socket and if necessary turn on the power at the outlet socket.

3 The OfficeConnect Remote performs a self test and loads the software. During the self test and software loading the ALERT and POWER LEDs flash.

Connecting to Your 10BaseT LAN

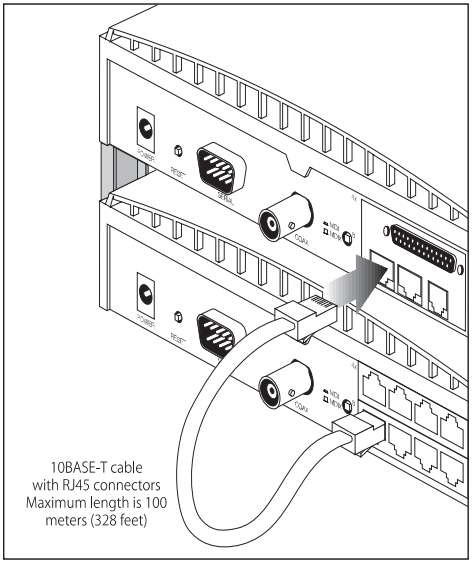


Figure 1-4 Connect The UTP Cable To OfficeConnect hub

You can connect the OfficeConnect Remote to a hub using 10BaseT cable in the following way:

1 Connect the UTP cable (not supplied) to the 10BaseT port of the OfficeConnect Remote.

2 Connect the other end to a 10BaseT port on your hub.

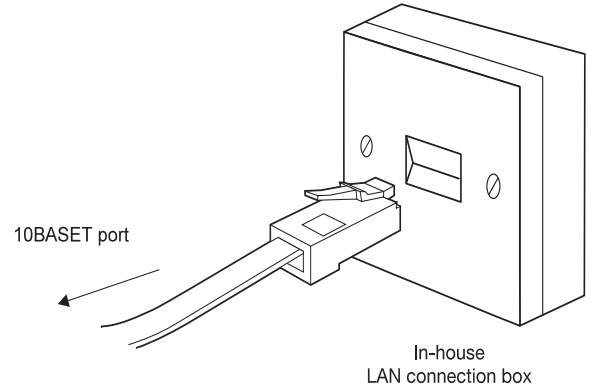


Figure 1-5 Connect The UTP Cable To In-House Lan Connection Box

To connect the OfficeConnect Remote to in-house LAN:

1 Connect the UTP cable (not supplied) into RJ45 socket marked LAN on the OfficeConnect Remote.

2 Connect the other end of the cable into the female socket of the in-house LAN connection box, as shown in Figure 1-5, or directly to a 10BaseT hub port.

Connecting to a Single Workstation

To connect the OfficeConnect Remote to a single personal computer or workstation:

1 Implement the crossover for the 10BaseT port on the OfficeConnect Remote by setting the MDI/MDIX switch to MDIX (out).

2 Connect the UTP cable (not supplied) directly into the RJ45 socket marked LAN on the OfficeConnect Remote.

3 Connect the other end to the 10BaseT socket on the workstation's Ethernet adapter.

Connecting to Your 10Base2 LAN

You can use the10Base2 Coaxial port to connect to your network and to other OfficeConnect units.

When using 10Base2 cable, it is important that both ends of the segment are properly terminated with 50 Ohm end pieces.

Only use 50 Ohm 10BaseT cables and use a 'Y' piece for each unit to ensure adequate clearance of the other ports. Due to the small size of the unit, you may find that a traditional 'T' piece does not provide enough clearance to allow space for fingers and cables when units are stacked together.

1 Connect a 10Base2 'Y' piece to each OfficeConnect unit and every other device to be connected.

2 Daisy-chain each 'Y' piece with a length of 10Base2 coaxial cable to form a single segment as shown in Figure 1-6. Remember to terminate the two free ends of the segment by fitting end pieces.

To disconnect a 10Base2 cable, twist each connector counter-clockwise to unlock it and remove it.

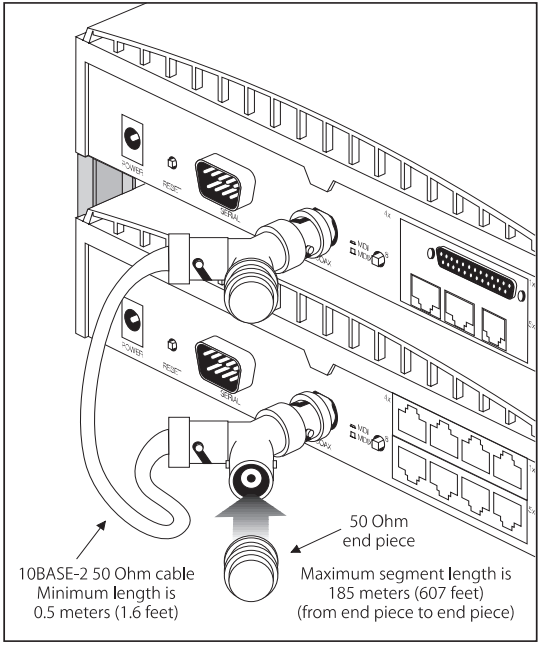


Figure 1-6 Connecting 10Base2 Cable

Connecting to ISDN

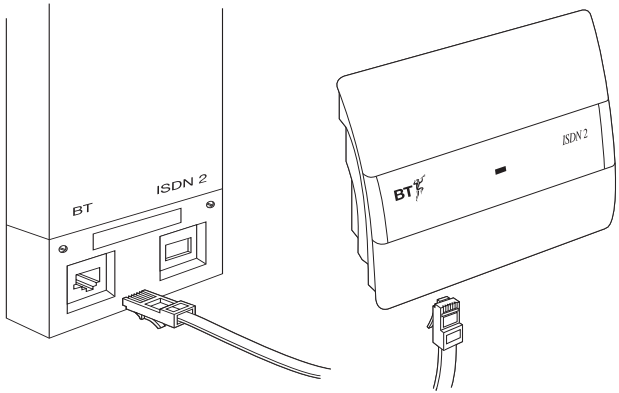


Figure 1-7 Connect ISDN Cable Into A Proprietary ISDN Wall Box

Connect the supplied ISDN cable from the ISDN port into the ISDN wall box (NT1). See Figure 1-7.

CAUTION: *Do not connect the ISDN line into the* OfficeConnect Remote*'s LAN port as the ISDN line voltage could damage the unit.*

Connecting to the WAN

If your OfficeConnect Remote unit is fitted with a WAN port, you can connect to a WAN Network Terminating Unit (NTU) fitted by your WAN service supplier. Using a suitable WAN cable (as described in Appendix B) connect one end to the WAN port on the OfficeConnect Remote unit and the other to the NTU.

Connecting to the VOICE Port

If your OfficeConnect Remote is fitted with a Voice port, then a standard telephone handset or other analog telephony equipment, such as a a fax or answering machine, can be connected to the port marked VOICE if required. This port can also be used to connect the OfficeConnect fax server to ISDN.

Some service providers offer Basic Rate ISDN connections with a single B-channel. If you connect a handset to a unit connected to this type of ISDN service, you cannot pass data while the voice port is in use. We recommend that you only connect voice equipment to ISDN services offering the standard 2 B-channel Basic Rate service.

The VOICE port is terminated with an RJ-11 socket. If your telephone equipment uses a different connector, you will need to obtain a suitable convertor to connect to the VOICE port. A British Telecom to RJ11 convertor is supplied with UK models fitted with a Voice port.

A dial tone is not provided to the handset if the ISDN line is not operational or has been disconnected.

Connecting a Management Terminal

Connect the Serial Manager cable to the Serial Manager port (marked Serial). Connect the other end to the serial COM port on your PC workstation.

When you have connected a management terminal, you can configure the Office Connect Remote to communicate with the remote site(s). See "Quick Configuration" overleaf.

Location of OfficeConnect Fax and Print Servers

If you are connecting the OfficeConnect Fax Server or Print Server to the OfficeConnect Remote, you must configure these units to operate with local servers only. If you do not do this, unnecessary ISDN calls are made, caused by the fax or print server polling the fax or print queue on remote servers at regular intervals (between once every 30 seconds to once a minute).

Quick Configuration

This section describes how you can configure the unit to bridge or route over ISDN links to suit most networking requirements using a simple forms-based user interface. If you want to connect to a remote site using leased line WAN links see "Setting Up a WAN Link" on page 1-29.

If you are unsure about the networking configuration you require, see "Examples of Typical ISDN Networking Applications" on page 1-31 for more information.

IMPORTANT *The Quick Configuration menu option is designed to be used only when you set up the unit for the first time. If you want to make any changes to the unit's configuration at a later stage, you should use the management system menus to make these changes. For more information, see the Software Reference guide.*

Starting Quick Configuration

1 Using a VT100 compliant terminal emulator, setup the terminal emulation to VT100 with communications parameters set as follows; select the COM port to be used for data transmission, 9600 bits/s – 8 data bits – 1 stop bit – no parity, with flow control set to none.

Example Using Windows 3.1 Terminal Application

Start the Windows 'Terminal' application. Using a mouse, click on *Settings* in the status bar to reveal the menu.

From the menu:

a Select the *Terminal Emulation* dialog box; confirm that *DEC VT-100 (ANSI)* is selected.

b Select the *Communications* dialog box; check the communications parameters are set as above.

c Select the *Terminal Preferences* dialog box; confirm that all check-boxes have been cleared.

Should the cursor disappear during configuration, confirm that the Cursor Blink check-box has been checked (i.e. shows a cross in it).

Should the keyboard arrow keys fail to move the cursor during configuration, confirm that the 'Use Function, Arrow, and Ctrl Keys for Windows' check-box has not been checked.

d Now save this configuration as a Windows terminal emulator file for future use.

If you are using Windows 95, use the Hyperterminal application and configure it in the same way as described above.

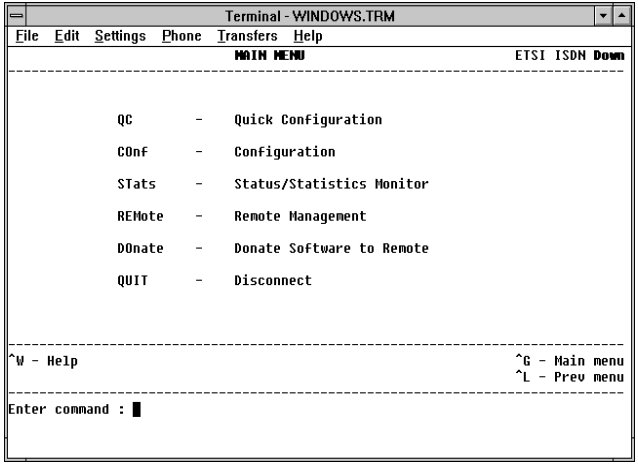


Figure 1-8 The Main Menu Screen

2 If the terminal emulator has been correctly configured, pressing [RETURN] displays the Enter Password screen.

3 Enter the default password, **PASSWORD** using uppercase characters. The Main Menu appears as shown in Figure 1-8.

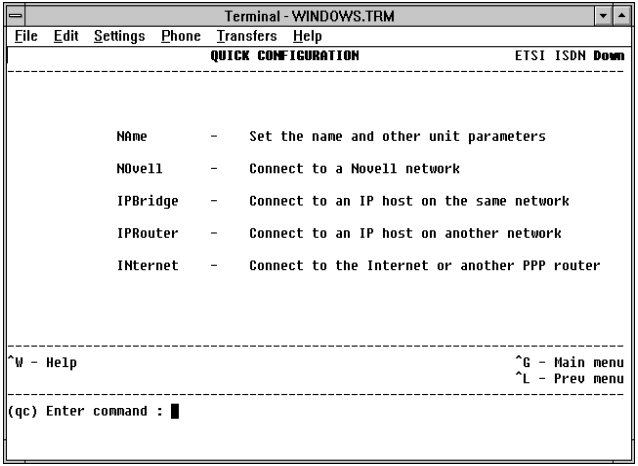

Terminal - WINDOWS.TRM
File Edit Settings Phone Transfers Help
QUICK CONFIGURATION
ETSI ISDN Down
NAme - Set the name and other unit parameters
NOvell - Connect to a Novell network
IPBridge - Connect to an IP host on the same network
IPRouter - Connect to an IP host on another network
INternet - Connect to the Internet or another PPP router
^W - Help
^G - Main menu
^L - Prev menu
(qc) Enter command :

Figure 1-9 Quick Configuration Menu

4 At the command prompt enter **QC**

The screen changes to display the Quick Configuration menu shown in Figure 1-9.

About Quick Configuration

You can configure the unit to connect to other Novell networks, to bridge to hosts on the same IP network (a network with the same IP network address), to route to a different IP network (an IP network with a different IP network address) and to connect to the Internet or other Point-to-Point Protocol (PPP) router. By using the commands several times, you can configure the unit to automatically connect to a combination of the above networks or to several different networks of the same type.

For example, if you need to connect to an IPX site, an IP host on a different network and to the Internet using an ISDN connection to your Internet service provider you would do the following.

- Use the **NO** command to configure the connection to the Novell server at the remote site.
- Use the **IPR** command to configure the connection to the remote IP host.
- Use the **IN** command to configure the connection to your Internet service provider's router.

You cannot configure the unit to be an IP bridge and IP router at the same time.

The OfficeConnect Remote talks to other OfficeConnect Remote units using its own very efficient FastConnect protocol over the ISDN or WAN port connections. If you need to communicate with another manufacturer's equipment, then you need to configure the OfficeConnect Remote to use the PPP protocol using the *Internet* option. See later in this section for more information. You can further configure the PPP parameters using the management system. See the *Software Reference* guide for more information.

Before configuring the unit to use PPP, you should check with your Internet service provider or with the system administrator of the remote site to find out which PPP parameters should be set and what their values should be. **Do not** *attempt to configure the unit to use PPP without this information.*

Setting the Unit Name

Before you configure the unit to connect to any other network, you must first give the unit a name. Enter **NA** at the command prompt on the Quick Configuration screen to display the screen illustrated in Figure 1-10.

The fields on this screen are:

Unit Name Type in a suitable name for this unit. The name can be up to 12 characters long, must contain no spaces and should, where possible, give an indication of the geographical location of the unit or the name of the users.

Manager LAN IP Address Type the IP address for this unit. It must be a unique IP address on your network.

Manager LAN IP Mask Enter an appropriate IP subnet mask. See "Subnet Masking" in Appendix A for more information about subnet masks.

Network Type Toggle the network type to match the ISDN service provided by your ISDN service provider.

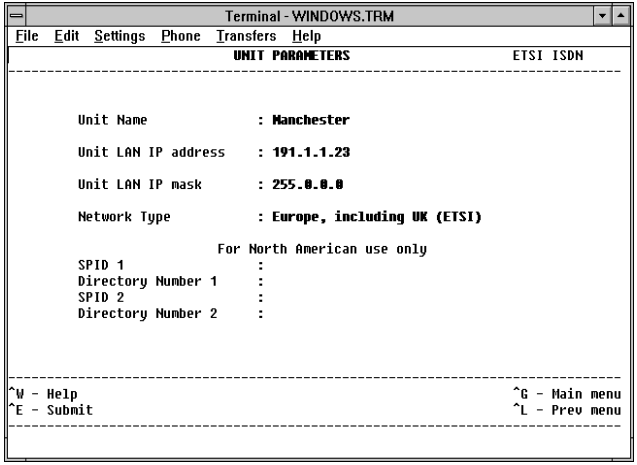

Terminal - WINDOWS.TRM
File Edit Settings Phone Transfers Help
UNIT PARAMETERS ETSI ISDN
Unit Name : Manchester
Unit LAN IP address : 191.1.1.23
Unit LAN IP mask : 255.0.0.0
Network Type : Europe, including UK (ETSI)
For North American use only
SPID 1 :
Directory Number 1 :
SPID 2 :
Directory Number 2 :
^W - Help
^E - Submit
^G - Main menu
^L - Prev menu

Figure 1-10 Setting The Unit Name

SPID 1 and 2 Service Profile IDs (SPID) are used by some ISDN service providers in the USA. If SPID is used, enter the value you are given by your ISDN service provider. Leave this field blank if you have not been provided a SPID.

Directory Number 1 and 2 Enter the ISDN number associated with each SPID.

Press [CTRL]+[E] to submit these parameters.

Connecting to a Novell (IPX) Network

To connect to a Novell network using FastConnect, enter **NO** at the command prompt on the Quick Configuration screen to display the screen illustrated in Figure 1-11.

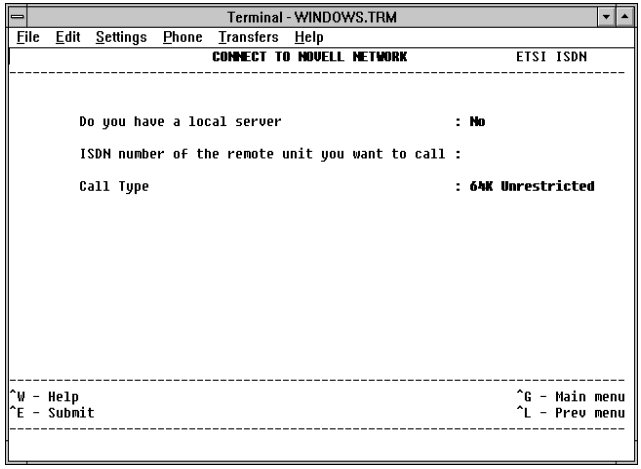

Terminal - WINDOWS.TRM
File Edit Settings Phone Transfers Help
CONNECT TO NOVELL NETWORK ETSI ISDN
Do you have a local server : No
ISDN number of the remote unit you want to call :
Call Type : 64K Unrestricted
^W - Help
^E - Submit
^G - Main menu
^L - Prev menu

Figure 1-11 Connecting To A Novell Network

Complete the fields on this screen as follows:

Do you have a local server? Use the [Spacebar] to toggle this field to Yes or No as appropriate.

If you have a local server, the unit's configuration is updated to ensure that no data destined for local servers is passed over the link

Remote ISDN Number Type the ISDN number of the remote unit that connects to the Novell network.

Call Type Set the Call Type for each ISDN number. Use *64k Unrestricted* for Euro ISDN lines. Use *56k V.110* or *56k_restricted* in the USA depending on the requirements of your ISDN service provider.

Press [CTRL]+[E] to submit this information.

When you do this the unit automatically makes a short call to the remote unit to interrogate the remote network for information about its servers. When it has obtained the information it needs the call is automatically disconnected. The unit then updates the autocall table so that when data is destined for a remote server, the unit automatically dials the correct ISDN number and connects to the remote network.

Enter **SAVE** at the command prompt to permanently store this configuration in the unit's memory.

Connecting to an IP Host on the Same IP Network

To connect to an IP host on the same network using FastConnect, enter **IPB** at the command prompt on the Quick Configuration screen to display the screen illustrated in Figure 1-12.

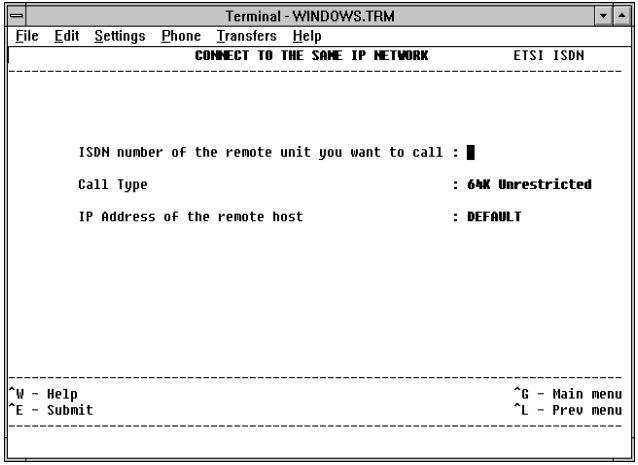

Terminal - WINDOWS.TRM
File Edit Settings Phone Transfers Help
CONNECT TO THE SAME IP NETWORK ETSI ISDN
ISDN number of the remote unit you want to call :
Call Type : 64K Unrestricted
IP Address of the remote host : DEFAULT
^W - Help
^E - Submit
^G - Main menu
^L - Prev menu

Figure 1-12 Connecting To An IP Host On The Same Network

Complete the fields on this screen as follows:

Remote ISDN Number Type the ISDN number of the remote unit that connects to the IP network.

Call Type Set the Call Type for each ISDN number. Use *64k Unrestricted* for Euro ISDN lines. Use *56k V.110* or *56k_restricted* in the USA depending on the requirements of your ISDN service provider.

Remote IP Address Type the IP address of the remote IP host to which you want to connect.

Press [CTRL]+[E] to submit this information.

An entry is made in the autocall table so that if any data destined to the remote host, a call is made automatically and a connection made to the remote IP network.

Enter **SAVE** at the command prompt to permanently store this configuration in the unit's memory.

Although calls to the remote site are only generated when data is addressed to a specific IP host or hosts (in our example, 191.000.000.100), any data that cannot be identified as local is also passed over the link while it is open. This can prevent the link from closing after the intended data has been transferred.

To avoid this situation you can also configure the units at both ends of the link to implement a Firewall and/or set the *Maximum Call Duration* in the ISDN parameters screen to reduce the amount of traffic permitted to pass across the link. See the *Software Reference* guide for more information about these features.

Alternatively, you may wish to configure the unit to operate as a router to prevent this problem occurring altogether. However, this requires that each site consists of separate subnets. See the next section for more information.

Connecting to an IP Host on a Different IP Network

To connect to an IP host on a different network using FastConnect, enter **IPR** at the command prompt on the Quick Configuration screen to display the screen illustrated in Figure 1-13.

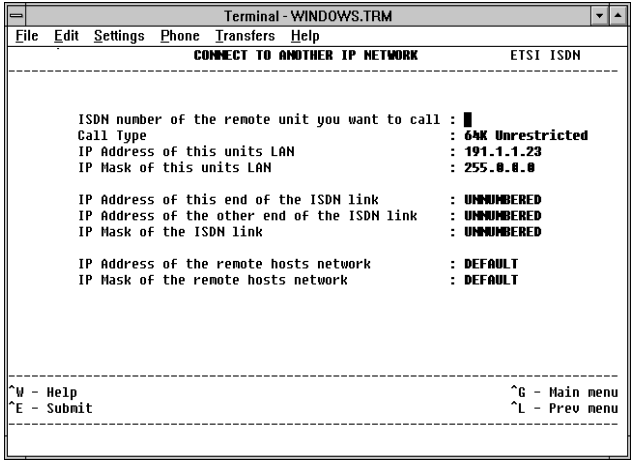

Terminal - WINDOWS.TRM
File Edit Settings Phone Transfers Help
CONNECT TO ANOTHER IP NETWORK ETSI ISDN
ISDN number of the remote unit you want to call :
Call Type : 64K Unrestricted
IP Address of this units LAN : 191.1.1.23
IP Mask of this units LAN : 255.0.0.0
IP Address of this end of the ISDN link : UNNUMBERED
IP Address of the other end of the ISDN link : UNNUMBERED
IP Mask of the ISDN link : UNNUMBERED
IP Address of the remote hosts network : DEFAULT
IP Mask of the remote hosts network : DEFAULT
^W - Help
^E - Submit
^G - Main menu
^L - Prev menu

Figure 1-13 Connecting to an IP Host on a Different Network

Complete the fields on this screen as follows:

Remote ISDN Number Type the ISDN number of the remote unit that connects to the remote IP network.

Call Type Set the Call Type for each ISDN number. Use *64k Unrestricted* for Euro ISDN lines. Use *56k V.110* or *56k_restricted* in the USA depending on the requirements of your ISDN service provider.

IP Address of this unit's LAN Type the IP address of this unit. This the address you entered on the Name screen.

IP Mask of this unit's LAN Type the IP subnet mask you entered for this unit on the Name screen. See Appendix A for more information about subnet masks.

IP Address of this end of the ISDN link By default this field is set to UNNUMBERED which allows unnumbered links to be used. This options is suitable for most network configurations. See Appendix A for more information about numbered and unnumbered links.

If you want to use numbered links, you must enter an IP address for this port that is on a different network or subnetwork than the unit's IP address.

IP Address at the other end of the ISDN link By default this field is set to 0.0.0.0 indicating unnumbered links are being used. If you are using numbered links, type the IP address of the remote ISDN port on the unit to which you want to connect. It must be on the same network or subnetwork as the local ISDN port.

IP Mask of the ISDN Link If you are using unnumbered links, leave this field set to 0.0.0.0. If you are using numbered links, type a subnet mask suitable use with the IP addresses you have selected for the ISDN ports at both ends of the link. See Appendix A for more information about subnet masks.

IP Address of the Remote Host Type the IP address of remote host to which you want to connect.

Remote IP Mask Type an IP subnet mask to match the address type being used. See Appendix A for more information about subnet masks.

Press [CTRL]+[E] to submit this information.

An entry is made in the autocall table so if any data destined to the remote host, an automatic call is made and a connection made to the remote IP network.

Enter **SAVE** at the command prompt to permanently store this configuration in the unit's memory.

Connecting to the Internet or a PPP Router

To connect to an Internet router or to a router using Point-to-Point Protocol (PPP), enter **IN** at the command prompt on the Quick Configuration screen to display the screen illustrated in Figure 1-14.

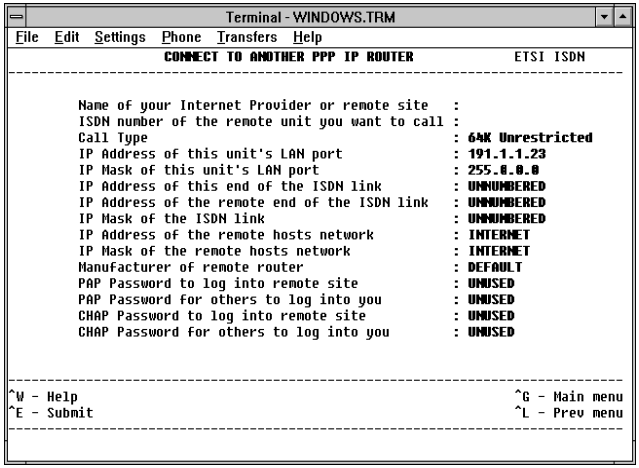

Terminal - WINDOWS.TRM
File Edit Settings Phone Transfers Help
CONNECT TO ANOTHER PPP IP ROUTER ETSI ISDN
Name of your Internet Provider or remote site :
ISDN number of the remote unit you want to call :
Call Type : 64K Unrestricted
IP Address of this unit's LAN port : 191.1.1.23
IP Mask of this unit's LAN port : 255.0.0.0
IP Address of this end of the ISDN link : UNNUMBERED
IP Address of the remote end of the ISDN link : UNNUMBERED
IP Mask of the ISDN link : UNNUMBERED
IP Address of the remote hosts network : INTERNET
IP Mask of the remote hosts network : INTERNET
Manufacturer of remote router : DEFAULT
PAP Password to log into remote site : UNUSED
PAP Password for others to log into you : UNUSED
CHAP Password to log into remote site : UNUSED
CHAP Password for others to log into you : UNUSED
^W - Help
^E - Submit
^G - Main menu
^L - Prev menu

Figure 1-14 Connecting To The Internet Or PPP Router

Complete the fields on this screen as follows:

If you are connecting to the Internet, your service provider will be able to give you the correct values for each of these fields.

If you are connecting to a remote PPP router, check with the system administrator of the remote network for the correct values for these fields.

Name of your Internet Provider or remote site Type the name of your Internet service provider or of the remote unit that connects to the remote IP network.

ISDN Number of the remote unit Type the ISDN number of the remote unit that connects to the remote IP network.

Call Type Set the Call Type for each ISDN number. Use *64k Unrestricted* for Euro ISDN lines. Use *56k V.110* or *56k_restricted* in the USA depending on the requirements of your ISDN service provider.

IP Address of this unit's LAN Type the IP address of this unit. This the address you entered on the Name screen.

IP Mask of this unit's LAN Type the IP subnet mask you entered for this unit on the Name screen. See Appendix A for more information about subnet masks.

IP Address of this end of the ISDN link By default this field is set to *UNNUMBERED* which allows unnumbered links to be used. This options is suitable for most network configurations. See Appendix A for more information about numbered and unnumbered links.

If you want to use numbered links, you must enter an IP address for this port that is on a different network or subnetwork than the unit's IP address.

If you are routing IPX using PPP, you must use numbered links.

IP Address at the other end of the ISDN link By default this field is set to *UNNUMBERED* indicating unnumbered links are being used. If you are using numbered links, type the IP address of the remote ISDN port on the unit to which you want to connect. It must be on the same network or subnetwork as the local ISDN port.

IP Mask of the ISDN Link If you are using unnumbered links, leave this field set to 0.0.0.0. If you are using numbered links, type a subnet mask suitable use with the IP addresses you have selected for the ISDN ports at both ends of the link. See Appendix A for more information about subnet masks.

IP Address of the Remote Host Type the IP address of a host on the remote network to which you want to connect.

IP Mask of the remote host's network Type an IP subnet mask to filter connections to inappropriate hosts. See Appendix A for more information about subnet masks.

Make of remote router This option sets PPP parameters needed to connect to the remote unit in its default configuration. If the remote unit's PPP configuration has been altered, you will need to amend the PPP parameters on this unit to reflect the changes. Refer to the *Software Reference* guide for more information

Toggle this field to the type of remote router to which you are connecting. The PPP options for the default settings at the remote router are then automatically configured when you press [CTRL]+[E] to exit this screen. The options are:

- Default – Use this option if you are connecting to another OfficeConnect Remote. Also use this option if the remote unit is none of the following and amend the PPP parameters accordingly.

- 3Com – 3Com NETBuilder router.
- Cisco – Cisco router.
- Ascend – Ascend router.
- Spider – Spider/Shiva router.

If you are connecting to a Spider/Shiva router, you need also to edit the ISDN port's configuration and set the PAP field in the LCP Configuration screen to Incoming. See the Software Reference guide for details.

PAP Password to login to Remote Site By default this is set to UNUSED. If you need to use a PAP password, enter the password provided by your Internet service provider or the system administrator responsible for the remote router. This password is submitted to the remote unit for it to verify. The password is case-sensitive.

PAP Password for others to login to you By default this is set to UNUSED. If you need to use a PAP password, enter the password provided by your Internet service provider or the system administrator responsible for the remote router. Your unit verifies that the remote unit is valid by comparing its submitted PAP password with the entry in this field. The password is case-sensitive.

CHAP Password to login to Remote Site By default this is set to UNUSED. If you need to use a CHAP password, enter the password provided by your Internet service provider or the system administrator responsible for the remote router. This password is submitted to the remote unit for it to verify. The password is case-sensitive. To ensure security, it is recommended that the local password is different from the remote password.

CHAP Password for others to login to you By default this is set to UNUSED. If you need to use a CHAP password, enter the password provided by your Internet service provider or the system administrator responsible for the remote router. Your unit verifies that the remote unit is valid by comparing its submitted CHAP password with the entry in this field. The password is case-sensitive.

Press [CTRL]+[E] to save this information.

An entry is made in the autocall table so that if any data destined for the Internet or Remote PPP routed network, a call is made automatically and a connection made to the remote router.

Enter **SAVE** at the command prompt to permanently store this configuration in the unit's memory.

Monitoring ISDN Line Usage

After you have first configured the unit for use with ISDN, it is important to monitor ISDN line usage to ensure that the unit is working in the way you expect.

Check the ISDN 1 and ISDN 2 LEDs to ensure that unexpected calls are not being made or that connections are not remaining open when you expect them to have closed.

Even if the ISDN Utilization LEDs are not lit, call with little or no data transfer may be in progress depending on how you have connected or configured the unit. As in a conventional telephone call, charges are made regardless of what is sent down the line until the call is dropped.

If you want to ensure that ISDN line usage is limited, set up ISDN Timebands or set the *Maximum Call Duration* parameter. See the *Software Reference* guide for more information on these features.

Setting Up a WAN Link

If you are using the OfficeConnect Remote to connect to a remote site over a leased line link, the initial setup is very simple.

1 Before you power on the unit, connect an appropriate WAN cable to the WAN port on the rear of the unit. If you have already powered on the unit, switch it off and connect the cable.

For more information about suitable cables, see Appendix B.

2 Power on the unit.

The OfficeConnect Remote automatically configures the WAN port to the appropriate line speed.

3 Refer to the *Software Reference* guide and edit the WAN port's configuration as follows:

a From the main menu, enter **CO PO**.

b Highlight the WAN port.

c Enter **ED** to display the Edit WAN Port screen shown in Figure 1-15.

d If you are routing, edit the Port IP address to set it to UNNUMBERED or to a valid IP address for the WAN link.

See Appendix A for more information about using numbered and unnumbered links.

If you are bridging, leave this field at the default setting.

e If necessary, change any of the other parameters to suit your WAN link. In most cases the defaults can be used.

f Press [CTRL]+[E] to submit this configuration.

The WAN port is now configured and provided the remote unit's WAN port has also been configured, data will be passed across the link.

Enter **SAVE** at the command prompt to permanently store this configuration in the unit's memory.

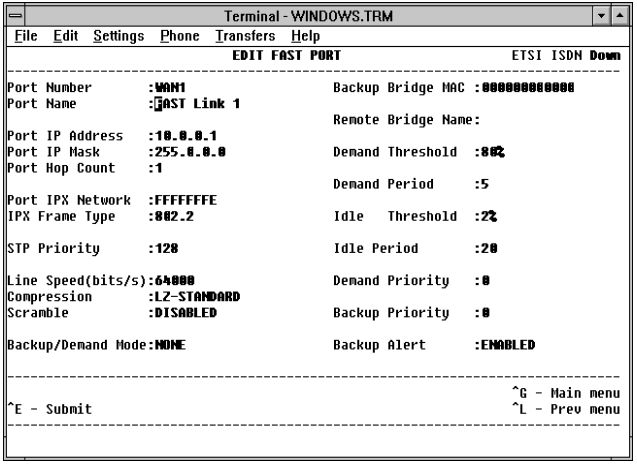


Figure 1-15 Edit WAN Port Screen

Examples of Typical ISDN Networking Applications

This section describes four of the most common applications of the OfficeConnect Remote. All of these configurations can be carried out using the *Quick Configuration* option and no further configuration is necessary to make the unit operational. However, you may want to fine tune the performance of the OfficeConnect Remote. The information provided in the *Software Reference* guide will help you do this.

The four typical applications are:

- Connecting to a Novell Network.
- Connecting to an IP host on the same IP network.
- Connecting to an IP host on another IP network.
- Connecting to the Internet or a PPP router.

You may need to combine two or more of these applications to provide full connectivity to your network. This is easily done by repeating the *Quick Configuration* option as many times as is needed.

Novell Network

Many organizations base their local area networks on Novell NetWare servers and users may need to access information stored on servers in other locations. If you are using ISDN to connect to the remote site, you can configure the OfficeConnect Remote to automatically call and connect to remote Novell servers when connection is required.

During configuration, once you have entered the ISDN number for the remote site, the OfficeConnect Remote makes a call to the remote site and autodiscovers the Novell servers on that network. It is then able to autocall the remote site whenever a connection to one of the remote servers is requested. To the user at the local site it will appear as though the server is on the same network.

When no data is being passed between the workstation and server, the OfficeConnect Remote closes the ISDN connection and the units at each end of the link *spoof* the Novell IPX protocol so that both the workstation and server believe the connection is still valid. As soon as the unit identifies that data needs to be passed to the server, the ISDN connection is re-established without the user being aware of ever being

disconnected. In this way ISDN calls are kept to a minimum.

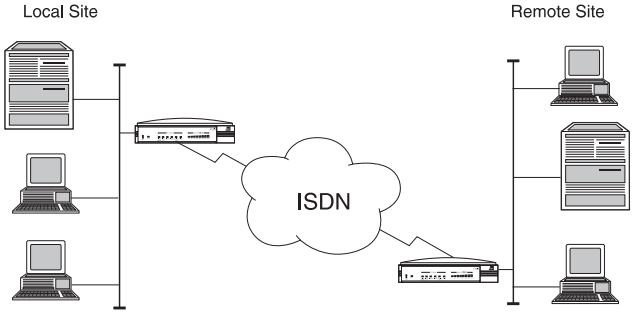


Figure 1-16 Connecting to a Remote Novell Network

In the example shown in Figure 1-16, the Local Site is connected to a Remote Site. The Local Site shown has several workstations and a server but could equally consist solely of workstations or even a single workstation (such as in the case of a homeworker). The Remote Site may be a central site for an organization or simply another like-sized office.

If you are connecting to the remote site over a WAN leased line link, the OfficeConnect Remote has no need to spoof the IPX protocol as there is a permanent connection in place. Once the OfficeConnect Remote has determined that the server is on the Remote Site all data between the server and workstation is passed over the link.

IP Host on the Same IP Network

If your organization operates a TCP/IP network and needs to extend the IP network over geographically remote sites, it is possible to bridge the network using the OfficeConnect Remote. It is only possible to bridge where both sites have the same network address and the devices are on the same subnet. In a class C IP address, the network address is the first three groups of numbers. For example:

`192.000.000.xxx`

where `xxx` represents the host ID of the individual devices on the subnet. See "IP Addresses" in Appendix A for more information about addresses.

Typically IP bridging would be used to connect a back office or home office into a main site. Any further network connections would be carried out from the main site. An example of such a network is shown in Figure 1-17.

During configuration, you enter the ISDN number and the IP addresses of any hosts to which you want to connect. In the example in Figure 1-17, the IP address of the host 191.000.000.100 is used and only when data destined for this device is received by the OfficeConnect Remote, is a call made to the remote site.

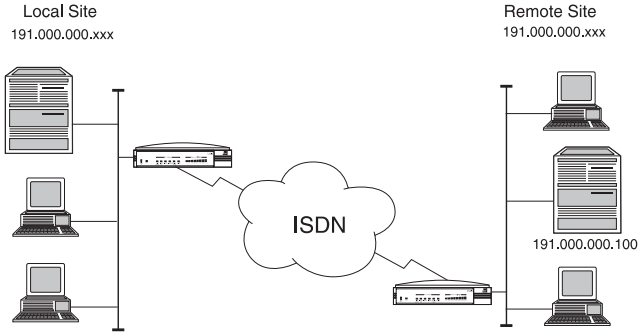


Figure 1-17 IP Bridged Network

There are some issues about which you should be aware when implementing an IP bridging solution.

- Although calls to the remote site are only generated when data is addressed to a specific IP host or hosts (in our example, 191.000.000.100), any data that cannot be identified as local is also passed over the link while it is open. This can prevent the link from closing after the intended data has been transferred.
- Some devices and applications (for example autodiscovery programs on SNMP managers) poll all devices on a subnet at regular intervals and this could lead to frequent ISDN calls if you have entered

several IP hosts to generate autocalls to the remote site. When combined with the problem described above, you could find your ISDN line permanently connected.

To avoid this situation you need to be sure that no devices or applications exist on your local site that could make unnecessary and costly calls to your remote site. You can also configure the OfficeConnect Remote units at both ends of the link to implement a Firewall and/or Call Guillotine to reduce the amount of traffic permitted to pass across the link. See the *Software Reference* guide for more information about these features.

Alternatively, you may wish to configure the OfficeConnect Remote to operate as a router to prevent this problem occurring altogether. This however requires that each site consists of separate subnets. See the next section for more information about IP routing.

IP Host on Another IP Network

Most organizations using TCP/IP protocols on their network, choose to subnet remote sites or even to have them on different networks. This requires that connections to remote sites are routed rather than bridged. The advantage of routing over bridging is that calls to the remote site are only made when data is specifically addressed to a remote network. Bridging passes any data not known to be for the local network to the remote network whether that is its destination or not.

Because the ISDN number can be associated with a remote network rather than just a specific IP host, any data for the remote network can generate an autocall and be routed over the OfficeConnect Remote. If you need to connect to IP hosts on several networks, you will need to use routing to be able to communicate with the different hosts.

The example shown in Figure 1-18 shows the Local Site connected to two Remote sites over ISDN. All sites are connected using OfficeConnect Remote units.

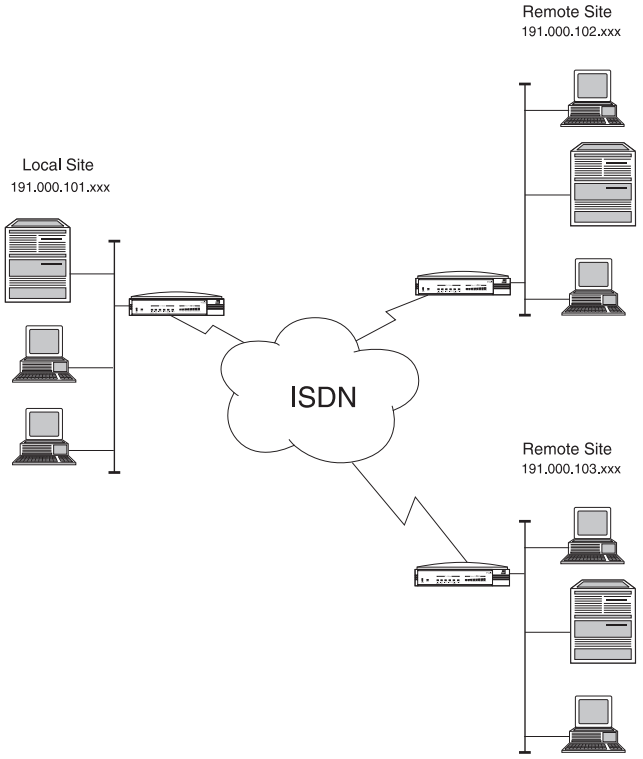


Figure 1-18 IP routed network

Internet or PPP Router

Some small businesses need high-speed connections into the Internet or need to connect to large global networks used by larger organizations. When communicating with another OfficeConnect Remote, the unit uses FastConnect, its own proprietary high speed protocol. However, in order to connect with other routers it needs to be configured to use the slower PPP protocol. PPP is used by many other routers.

Increasingly Internet service providers are offering access to the Internet over ISDN via an ISDN router. PPP routing over ISDN allows a simple cost-effective connection to the Internet or into a large organization's global network.

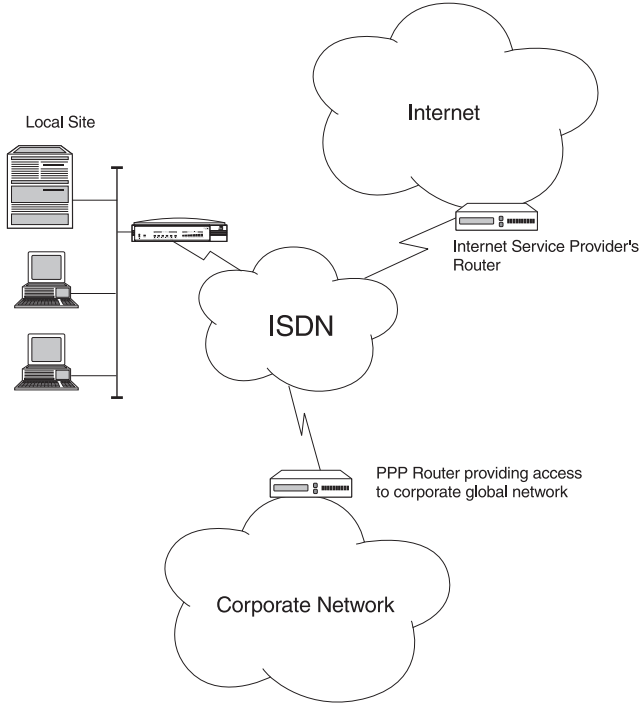


Figure 1-19 PPP Connections to the Internet and Corporate Network

Multiple Connections from a Single Site

In some instances it is likely that you will need to connect to Novell servers on one site, IP hosts on the same remote site or possibly a different remote site and a connection into the Internet. This can all be achieved by running the simple configuration several times until all the desired types of connection have been configured. The only thing you need to be aware of is that you cannot bridge and route the same protocol.

The local site shown in Figure 1-20 is a small business that needs data links to several of its clients and a connection to the Internet. It has an IPX connection to access information on one client's NetWare server and IP routed connections to several IP hosts at different clients' sites. Finally, there is a connection to the local Internet service provider's PPP router giving fast access to the Internet. All connections can be set up with an autocall so that connections to the remote sites are made as soon as the OfficeConnect Remote identifies data not destined for the local network.

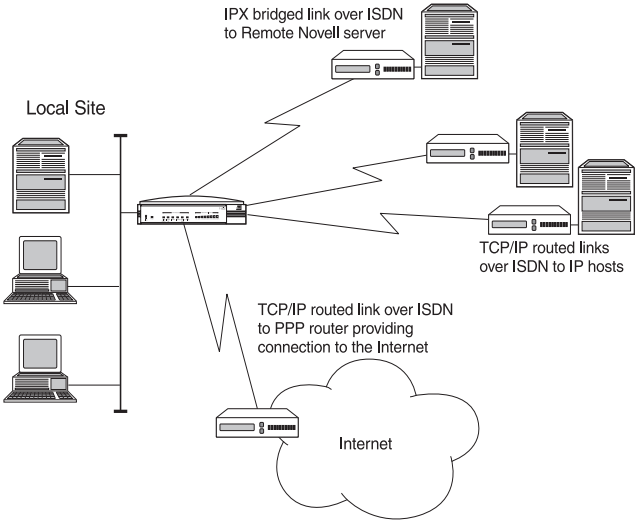


Figure 1-20 Multiple Connections from a Single Site

Troubleshooting

WARNING: *There are no user serviceable components inside the case of the unit.*

CAUTION: *Read the section 'Important Safety information', at the start of this manual.*

The OfficeConnect Remote is fully performance tested after assembly. Providing the unit has been correctly installed, and is used in accordance with the instructions contained in this manual, difficulties should not arise. If unit or system maintenance is required, then it must be carried out by a competent network engineer.

In the unlikely event that you experience problems with the unit, the following procedure will enable you to undertake basic troubleshooting before contacting your 3Com reseller.

Malfunction	Remedy
If you cannot connect your OfficeConnect Remote to the network or PC.	Verify that your computer is equipped with an available serial port and that the correct cables and connectors are being used. If in doubt contact the unit's supplier.
The POWER LED does not light.	Confirm that: a) The switched outlet socket of the electrical mains system supply is turned on. The main lead is correctly plugged into the unit's electrical mains system inlet socket. b) The switched outlet socket is 'live' by plugging the unit into an alternate socket to see if it functions.

Malfunction	Remedy
The ISDN OK LED does not light.	Follow the procedures as outlined for "The POWER LED does not light." a) Ensure that the OfficeConnect Remote is powered up and the POWER LED is lit. b) Confirm that the ISDN UTP cable is correctly connected, and that the cable is attached to the socket marked ISDN. c) Confirm that the ISDN line socket that is connected to the unit is conveying an ISDN service. d) Check that the ISDN port is configured using the **CO PO** command. See the *Software Reference* guide for more information about this command. e) Try making an ISDN call using a telephone connected to the ISDN line to confirm if the line is operational. f) If the LED still fails to light, plug the UTP cable into an alternate ISDN service socket to confirm that it functions. g) Try using an alternate UTP cable to connect the unit to the ISDN service socket.
If other LEDs do not light during operation of the unit.	During normal operation the remaining unit LEDs should light and extinguish depending on the action being taken. If the LEDs fail to light in accordance with their function (refer to "Front Panel" on page 1-6), then contact your supplying 3Com reseller.
The local unit does not connect to the remote unit.	a) Check the connections between the unit, the network, or PC and the ISDN line. b) Confirm that the line is working by connecting a telephone to the ISDN line to make a call. c) Check that the number which you are dialling is connected to the remote unit and that the unit is configured to be able to answer calls.

A BRIDGING AND ROUTING

Introduction

During the initial configuration of the OfficeConnect Remote you must decide whether to configure the unit as a bridge or as a router although we may help you with this choice with our Quick Configuration options. If you are unsure which option you should choose, read this appendix to help you decide.

Bridges and routers are used to connect networks together. The cost of connecting networks together is generally proportional to the distance over which the network extends and the amount of bandwidth required. Large amounts of bandwidth can be provided easily within a LAN by connecting different segments together with a local bridge. However, it becomes impractical and expensive to extend this bandwidth over larger distances, and it is, therefore, usual to interconnect local high speed networks using bridges or routers connecting over slower speed terrestrial and satellite links.

In the following sections we describe the concepts behind bridging and routing, and discuss the different ways in which LANs can be configured and operated to optimize performance and minimize disruption of traffic on each individual LAN.

Bridging and Routing Concepts

A bridge connects one or more LANs together. It examines each data frame received at a LAN port and forwards any frames that it assumes are for a destination device not connected to that LAN port. The bridge is able to do this by learning which devices are connected to each LAN port.

A router learns much more about the networks connected to it and is able to be much more selective about the data it passes on to other networks and to which networks it transmits. By default routers reject or *filter* data unless it matches predefined attributes (for example specific protocols or destination network addresses). In large interconnected networks a router selects the best route for data to travel.

Guidelines For Choosing Bridging or Routing

The list below outlines some of the reasons why you might choose to configure the OfficeConnect Remote as a bridge or a router. Read through the rest of this appendix for more explanation and to help decide which of the above conditions apply to your network.

- A bridge is simpler to configure but a router can provide more security on a busy network and filter unwanted data transmissions more effectively.
- If your network consists of only one or two links between different sites and your network is not heavily loaded, in most circumstances you can configure your OfficeConnect Remote units as bridges.
- If your network structure is complicated and consists of a mixture of leased line and ISDN links, or if it uses several different protocols, you may obtain better performance from the OfficeConnect Remote units if you configure them as routers.
- If you are connecting to a routed corporate network that is already running IP and/or IPX protocols or if you are using the OfficeConnect Remote to connect to the Internet you must configure the unit as a router.

How Bridges Learn

When a bridge is first powered on, it does not know the number or the locations of stations that are connected to the LAN. To minimize the amount of data passed over the bridge it must *learn* the whereabouts (address) of stations to ensure that it passes only the data that is intended to be passed over the bridge.

Like the envelope of a letter, the header of each frame of data transmitted on the network has a From (source) address and To (destination) address. This ensures that data reaches its destination on the LAN and that the receiving station can reply. The bridge reads every frame of data received at the LAN port and extracts the source address of the frame. From this information it builds an address table of stations it knows to be on the LAN.

To decide if data should be passed over the bridge, the bridge examines the destination address of the frame. If the address is already in its address table, the bridge knows the destination is on the LAN and therefore rejects or *filters* the frame.

If the destination address is not in the address table, the bridge transmits the data across the bridge. It does this even if the destination device is on the

local LAN because it does not recognize the destination station as local. However, if the destination device is on the local LAN, once it replies to the original source station, its own source address is part of the data frame and it is learned by the bridge and added to the address table.

By operating in this way, the amount of data forwarded by the bridge is kept to a minimum. Traffic that is for devices on the attached LAN is rarely forwarded over the bridge.

A bridge can be configured to forget or *age* a station's address after a period of inactivity, a facility which is used to ensure that stations which are no longer attached to the LAN, do not remain in the bridge's address table, using up space that may be required for other stations' addresses.

Some bridges allow address information to be manually configured into the bridge, provided the automatic *learning* facility is turned off, although this will not normally prove necessary unless specific traffic filtering is required.

You can also configure a number of other features to improve the performance and operation of the OfficeConnect Remote. These include sophisticated frame filtering techniques so that only certain types of frame, or those associated with particular work groups, are passed between specific segments.

Bridging Between Remote Sites

The OfficeConnect Remote is able to send frames between LANs that may be separated by considerable physical distances. It achieves this by making use of Wide Area Network (WAN) links. WANs can be established by using either digital leased lines or ISDN and are usually operated by telephone companies (PTTs) or other service providers.

Figure A-1 shows two LAN segments, A and B, which are connected by a pair of OfficeConnect Remote units, 1 and 2. The type of link between the two depends on the WAN services available at each of the remote bridge locations, and the price the network administrator is willing to pay for those services.

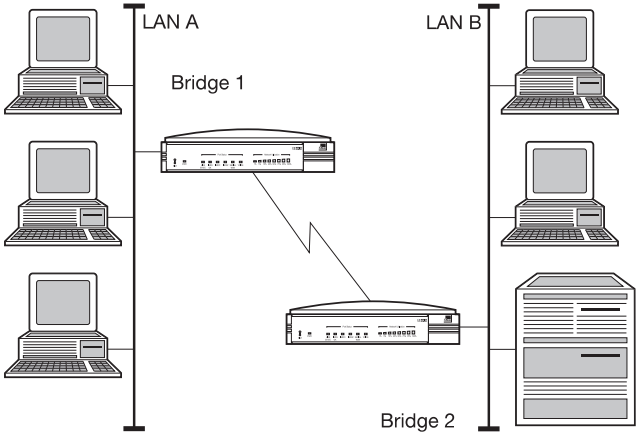


Figure A-1 Simple Remote Bridging

The OfficeConnect Remote uses FastConnect, its own protocol, to ensure the most efficient connection with other OfficeConnect Remote units. However, if you are connecting to a different type of bridge/router the standard PPP communications protocol is required to establish the link. You can configure outgoing calls to use either FastConnect or PPP as required. The ISDN port on the OfficeConnect Remote autosenses the protocol being used on incoming calls and switches to the protocol necessary for that connection.

If you are using ISDN to connect to different networks, the two B channels can be used independently to connect to different networks at the same time.

Building a Larger Network

Large networks of interconnected LANs can be established by using multiple bridges as illustrated in Figure A-2.

The bridges build up their address tables. If the destination unit is not registered as being accessed via the bridge's LAN interface, the frame will not be placed on LAN A. Therefore, frames passing between LAN B and LANs C or D will not impact the overall performance of the LAN.

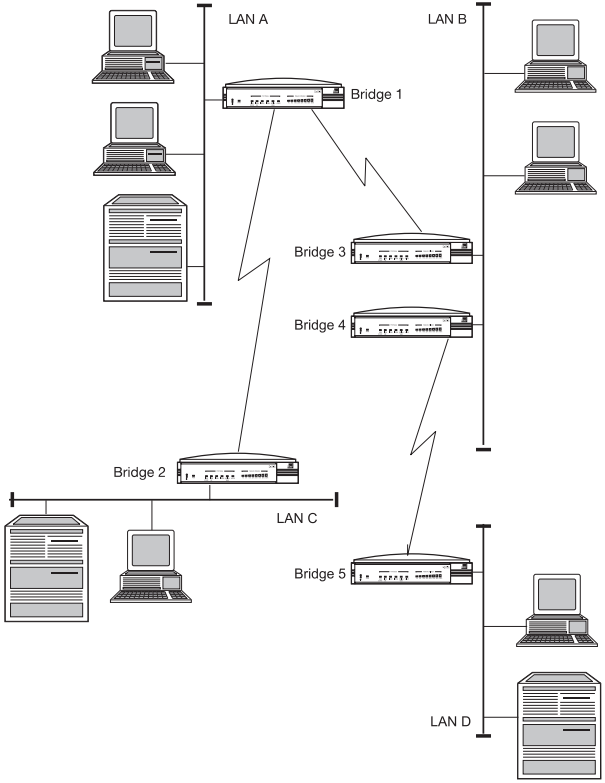


Figure A-2 Multiple Remote Bridges

Multiple Paths Between Bridged LANs

With only a single physical path between LANs, the network is susceptible to link and bridge failures. In the event of a failure, the connection between any of the LANs upstream or downstream of the point of failure will be broken. A more resilient network of interconnected LANs can be established by providing more than one link between any two of the LANs.

Normally, this network would soon encounter serious problems resulting from a loop, around which frames could endlessly travel if precautions aren't taken by the bridges. Over ISDN links a proprietary form of loop control is implemented. On WAN leased line links the Spanning Tree Protocol (STP) prevents data loops.

On startup, the bridges send out frames to enquire if there are other bridges on the network. By exchanging information, the bridges block ports that cause the loops and ensure that there is only ever one active path through the network. If one of the links or bridges fail, the other bridges detect this and reconfigure their ports so that there is once again an active data path through the network.

Network Topology

If your network topology is star shaped, a combination of ISDN and bridging is usually the most efficient and successful option. Routing is a better solution if your network topology is a complex mix of both leased line and ISDN circuits, running at 64 Kbps to 2 Mbps.

Broadcast Storms

Bridges are programmed to automatically forward data packets by default while routers filter data packets by default. These attributes have an impact on the overall flow of data across the network. Much has been made of *broadcast storms* in connection with bridged networks, where the broadcast signals from bridges propagate to fill all of the wide area bandwidth, and bring the network down. Broadcast storms cannot be attributed to installation of bridges or routers, but by poor protocol implementation and network design. However the deployment of routers can effectively *firewall* one logical network from another.

Optimum Use of Resource

Bridged networks use Spanning Tree Protocol (STP) to provide network resilience, by retaining redundant links on stand-by, in case the primary link fails. This means that you are not making maximum use of available resources.

Routing protocols make each node aware of the primary and alternate routes available, ensuring that resources (particularly WAN links) are not wasted.

Routers have been designed to provide the optimum route through the network from the workstation through to the destination resource with which the user wishes to communicate. In a very large network there could be multiple paths available, and these could change as dedicated links go in or out of service. These changes in network topology are handled by routing protocols. However, when using the ISDN the source network can dial direct to the destination network, and establish a point-to-point bridged or routed connection. Generally, when using this type of ISDN dial-up link, routing does not provide much extra benefit.

Network Organization, Structure and Physical Layout

Some organizations are structured into departments determined by the physical layout of their work environment, so it is natural to divide the corporate network into separate logical networks. Routing becomes the obvious candidate for handling these individual LANs.

The Internet

The protocol adopted by the Defense Data Network (DDN) for the Internet, is based on obtaining and abiding by, a registered Internet address range. This makes a router the ideal choice for accessing the Internet. Unfortunately, new applicants are likely to only get a *Class C* registered Internet address, preventing more than 254 connections on one bridged IP LAN.

Routing IP and IPX

Running a bridged network allows workstations to communicate directly between one another. A PC user wishing to communicate with a remote network server is totally unaware of any intervening bridges. This is known as transparent operation.

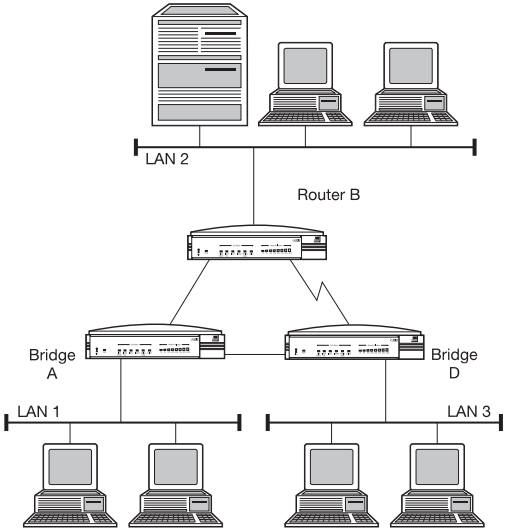


Figure A-3 Example Network

It is important to understand that in a bridged network the addressing structure for both IP and IPX relates to a single network. If the units in Figure A-3 were bridges and not routers, then an IP node on LAN A could, for example, have an address 140.56.10.0, the node on LAN B an address 140.56.10.2, and the node on LAN C, an address of 140.56.10.3. All the nodes, therefore, are able to share the same Class B network address, regardless of their location on the bridged network.

However, if there were NetWare nodes throughout the three bridged sites, they would also share the same IPX network number. If each of the bridged LANs supported a network server, each with its own unique network number, and an IPX address is misconfigured, the NetWare network server consoles will report the message 'Router Configuration Error – Router XXXXX claims that LAN is XX-XX-XX-XX'. (The router it refers to is in fact the network server).

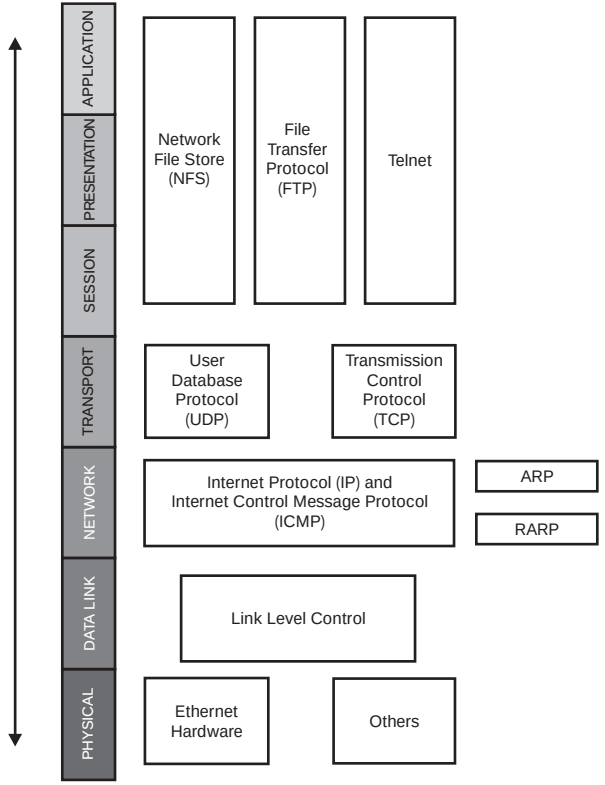


Figure A-4 Open Systems Interconnection Network Layer Model

A routing environment allows stations to communicate indirectly. Following the example in Figure A-3, let us assume that a station on LAN 1 wants to communicate with a network server on LAN 2. The station on LAN 1, constructs a *Layer 2* datalink header (see Figure A-5), with the source station's hardware address, and also the destination hardware address of the local router. To direct the packet to its final network destination, the source station must complete the *Layer 3* network header with the destination network address of LAN 2.

Once the packet is received by the Router A, attached to LAN 1, it strips off the network header (refer to Figure A-5) and examines the Layer 3 datalink header information. It then reviews its routing tables in order to establish where to forward the data packet. It is possible that the LAN 1 router has multiple outgoing ports that would allow different transmission routes to the destination network. In our example using Figure A-3, a packet could go via Router D to get to Router B, or it could go more directly across a single direct link between Router A and Router B.

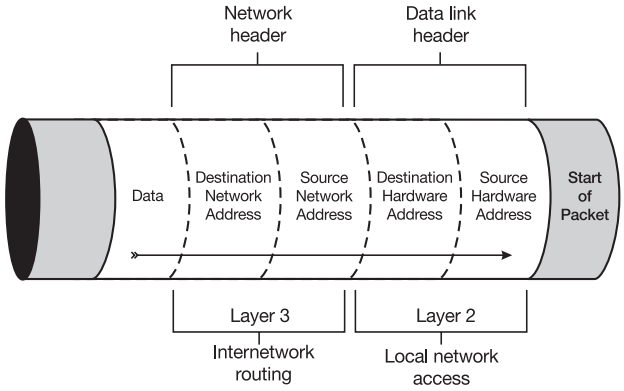


Figure A-5 Data Packet Containing Hardware And Software Addresses

IP Routing

The local router contains, within its routing table, information which will allow it to determine the best data transmission route. The type of information the router uses to make these assessments is protocol dependent, and some communications protocols may employ a range of routing algorithms, and accompanying routing protocols. In the case of the TCP/IP protocol suite, the OfficeConnect Remote utilizes the Routing Information Protocol (RIP). RIP is also known as a *distance vector* protocol.

Different protocols use differing network characteristics or *metrics* when making routing decisions. The metric employed by RIP is a *Hop Count*. A hop count is defined by the number of routing nodes there are between the source and destination units. In our example, there are two hops between LAN1 and LAN 2 going via Routers A and B. If traffic was directed via Routers A, D, and then B, this would be three hops.

The algorithm will automatically select to forward the data packet via Router A, as this route contains the least number of hop counts which makes it the preferred direct route.

Every thirty seconds, each IP router will advertise via RIP datagrams, to all other routers on the internetwork, how many hops it takes to reach all connected logical networks, based on the routers network position and the state of its physical links. In an ISDN environment, making ISDN calls every thirty seconds to pass on and receive RIP updates would be costly. When initially setting up the network, the OfficeConnect Remote is manually connected over the ISDN for a three minute period, in order to learn the topology of the rest of the network. Once this has been performed the OfficeConnect Remote will only make ISDN calls to transmit data packets. While this data transfer is in progress, RIP updates will be *piggybacked* on to the call, updating both parts of the network with the latest RIP information.

It is also possible to assign what are known as *static routes*, which are manually entered fixed routes. The network manager may be aware of specific traffic patterns, or needs to enforce a particular routing policy. Static routes provide an option to force traffic through the network in a particular way. The disadvantage with this approach is that routing protocols dynamically update all the routers on the network, with the current network topology, enabling backup routes to be deployed. In a static route situation, if the WAN links in that routing definition are down, then traffic cannot be passed. Implementing a static route prohibits the router from being able to offer alternative data paths.

IPX Routing

Novell IPX also uses RIP for routing purposes. Although it is similarly named to the IP equivalent, it uses a different protocol. IPX RIP broadcasts datagrams out onto the network every sixty seconds. Upon receipt of a RIP datagram, a router adds one to the hop count of each route advertised and broadcasts a RIP datagram to the other networks, with which it is connected.

The cost of a route in an IPX network is determined by the metric known as *ticks*. In a LAN only environment this is the hop count plus one, e.g. three hops or four ticks. For an internetwork connected via a WAN or ISDN links, the tick count is factored on the speed of the WAN link.

We saw above the common network numbering scheme employed for a bridged network. By employing routing, LAN A, LAN B and LAN C become three separate networks on a network. The network numbering must reflect that situation.

In a Novell IPX environment we could allocate IPX network numbers 00000111 to LAN A, 00000222 to LAN B and 00000333 to LAN C. Having configured the ports of the OfficeConnect Remote to accept this protocol, routing will now occur between the remote network servers and workstations but addressed by different network numbers.

It should be noted that NetWare 3.X and later, uses the concept of internal IPX addresses, which is somewhat similar to network addressing. The internal address refers to the internal network within that server allowing internal processes to communicate. These numbers must be unique for all servers right across the network. Although network servers may appeared wired correctly, and in other respects seem to be working correctly, duplicated internal IPX addresses will not allow correct operation.

NetWare has a hop count limitation imposed by the RIP. On an IPX network a data packet can cross a maximum of fifteen routers before being discarded.

IP Addresses

TCP/IP Numbering and subnet masking IP numbers or *addresses* are normally made up of four fields (normally called *bytes*), with each byte having a whole number value of between 0 and 255, and the bytes separated by a full stop. For example:

```
123.123.123.123
```

An IP address is divided into two sections, one is the *Network Address* section and the other is the *Host Address* section. For example:

```
123.123.|123.123
  Network      Host
```

The divider | between the two sections is moveable according to what *class* of IP address it is. The class of address is defined by what the number is in the first address byte:

- For a Class A IP address the number in the first byte will be in the range 00 to 126
- For a Class B IP address the numbers in the first & second bytes will be in the range 128.001 to 191.254
- For a Class C IP address the numbers in the first, second & third bytes will be in the range 192.000.001 to 223.255.254

For example:

```
Class A   1.|123.123.123
        Network      Host

Class B   128.001.|123.123
            Network      Host

Class C   192.123.123.|123
                Network      Host
```

Using of any of the address classes in a private TCP/IP network is not a problem, providing that connections outside of that private network to external public or private TCP/IP networks are never needed. If a private IP addressing number scheme is established within a private corporate network, connections out of that network to external public or other private TCP/IP networks, can be achieved via a computer which has software which enables it to act as an IP *gateway*. These devices, if configured correctly, provide the IP numbering/address translation between the two networks.

Subnet Masking

Subnet Masking is a mechanism which can be enabled in computer and communications equipment which tells the equipment and the network, which parts of the IP address are to be used as the *Network* identifier and which are the *Host* identifier.

A subnet mask consists of a similar field structure to that of the IP address (123.123.123.123). For example:

`255.255.0.0`

This means that the first two three digit bytes of the IP address (the fields *masked* by - 255.255) are to be recognized and used as the Network address, and the last two bytes (those set to .0.0) are to be used to identify the Host address.

An alternative way of expressing a subnet mask is a single number indicating how many bits of the IP address are to be used for the network address. For example 255.255.0.0 can be expressed as 16 while 255.255.255.192 can be expressed as 24.

The OfficeConnect Remote can be configured to use subnet masking to enable ISDN Autocalls to be made on groups of IP addresses or on specific IP addresses.

Normally, a subnet mask would be set so that any IP address, in a range of hosts on a destination LAN which are detected on the unit's locally connected LAN port, causes an ISDN Autocall to be made out to that destination.

This is achieved by the addition of a `/xx` number at the end of the configured address. For example:

`193.123.123.123/32`

The `/32` appended to the IP number indicates that all four of the bytes are used and must have valid entries.

A `/24` mask, for example:

`193.123.123.0/24`

means that only the first three bytes are to be recognized and used, and the last byte can be ignored. In this case, any IP address appearing on the locally connected LAN in the range 193.123.123.0 to 193.123.123.255 will cause an autocall to be made to the destination network who's name is associated with that number in the ISDN Autocall table. The name is then looked up in the ISDN Numbers table and a call made to the ISDN number which has been assigned to that name.

Obtaining an IP Address

If you want to use a unique IP addressing system on your network so you can connect to the Internet, there are three organizations responsible for allocating network addresses. These details are correct at the time of printing but may change.

USA - InterNIC, Network Solutions

Attention: InterNIC Registration Services
505 Huntmar park Drive
Herndon
VA 22070

Telephone: 1-800-444-4345 (Toll Free)
1-619-455-4600
1-703-742 4777

You can also send e-mail to these addresses:

- hostmaster@rs.internic.net
(host, domain, network changes and updates)
- action@rs.internic.net
(computer operations)
- mailserv@rs.internic.net
(automatic mail service)
- info@internic.net
(automatic mail service for general enquiries)
- refdesk@is.internic.net
(enquiries not handled by the services above).

Europe -RIPE

Attention: RIPE NCC
Kruislaan 409
NL-1098 SJ Amsterdam
The Netherlands

Telephone: +31 20 592 5065
Fax: +31 20 592 5090
e-mail: ncc@ripe.net

Asia Pacific Network Information Center (APNIC-DOM)

Attention: Asia Pacific Network Information Center (APNIC-DOM)
c/o Computer Center
University of Tokyo
2-11-16 Yahoi
Bunkyo-ku, Tokyo 113
Japan

Admin. Contact:	Nakayama, Masaya (MN89)
Telephone:	+81 3 3812 211 ext2720
e-mail:	nakayama@nic.ad.jp
Technical Contact:	Conrad, David (DC296)
Telephone:	81 3 3580 3781 or 3580
Fax:	81 3 3580 3782
e-mail:	davidc@apnic.net

Numbered and Unnumbered Links

When routing and using the OfficeConnect Remote's FastConnect protocol over ISDN or serial WAN links as opposed to PPP, you have the option of using numbered or unnumbered links.

A numbered link requires a valid IP address to be configured for both ports connected to each end of the link. The IP address used must be for a different subnet or network than that used by either LAN at each end of the link. An example is shown in Figure A-6. In this example, the Local Site uses the network address 191.000.100.xxx on its LAN. The remote site uses the network address 191.000.200 on its LAN and the link uses 191.000.300.

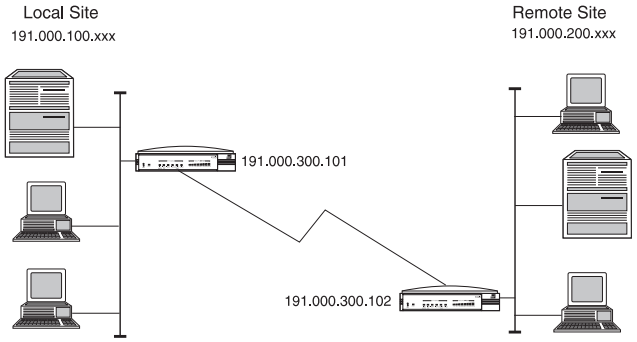


Figure A-6 Example of a Numbered Link

By default the WAN port and ISDN port have an IP address of 10.0.0.1. This is set to allow remote Telnet connections to the unit to enable configuration but must be changed when configuring the unit to allow correct operation. If you use the *Quick Configuration* (**QC**) option to configure the unit to operate over ISDN, the Port IP Address is set to unnumbered.

In most instances you should use unnumbered links. This is easier to configure and does not use network addresses which may be in short supply.

B TECHNICAL INFORMATION

Specifications

LAN Connector Interfaces

- 10Base2 via a coaxial connector.
- 10BaseT via an RJ45 connector socket for UTP.

Only one LAN connection can be used at a time

WAN Connector Interface

25-way D-type female connector, configured to support one of:

- V.11 (X.21) for speeds up to 2.048 Mbps.
- V.28 (V.24/RS232) for speeds up to 19.2 Kbps.
- V.35/V.36 for speeds up to 2.048 Mbps.

ISDN Connector Interface

Provides a twin interface to a 2B+D basic rate ISDN service, via an RJ45 connector socket.

Voice Connector Interface

Provides interface for analog telephony equipment via RJ11 connector socket. Adaptors may be required for some telephone equipment connections.

Management Connector Interface

9-way D-type connector for use with a VT100 compliant terminal or PC.

- Local and remote terminal management.
- TCP/IP Telnet menu driven management interface for remote management.
- Software upgrades, enhancements and configurations downloadable from network attached terminal or PC.
- SNMP MIB II support with private extensions for management of unique features.

Bridge Characteristics

- 802.3 MAC layer bridge.
- 802.1D spanning tree algorithm.
- Support for bridge triangulation and link load sharing.

Performance

- LAN filtering rate: 10000 frames per second.
- LAN forwarding rate: 4000 frames per second.

  ISDN and WAN forwarding rates are dependent on the link speed.

Approvals

This product ostensibly complies with the electro-magnetic compatibility (EMC) requirements of EN 55022 Class A and EN 50082 (susceptibility). However, to fully comply with Class B of EN55022 the following prerequisites should be observed:

- The WAN port must be attached to a screened digital cable.
- The ISDN cable must be used in conjunction with a three turn ferrite.

The product carries the *CE* certification mark to indicate conformance with the following EU directives:

- LVD (Low Voltage Directive (Safety) 73/23/EEC.
- EMC (Electro Magnetic Compatibility) Directive 89/336/EEC.
- TTE (Telecommunication Terminal Equipment) Directive 91/263/EEC.

  The product conforms to I-CTR3 (based on NET3 – ISDN interface).

FCC Requirement

This product has been verified to comply with the limits of Class B computing device pursuant to Subpart J of Part 15 of the FCC Rules.

WARNING: *This product generates and uses radio frequency energy and, if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio or television reception.*

The product has been tested and found to comply with the limits for a Class B computing device in accordance with the specifications of Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in a residential installation. However, the is no guarantee that interference will not occur in a particular installation.

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorientate the receiving antenna.
- Relocate the product away from the receiver.
- Plug the unit into a different outlet so that the computer and the receiver are in different branch circuits.
- Ensure that all product fixing screws, attachment connector screws and ground wires are tightly secured.

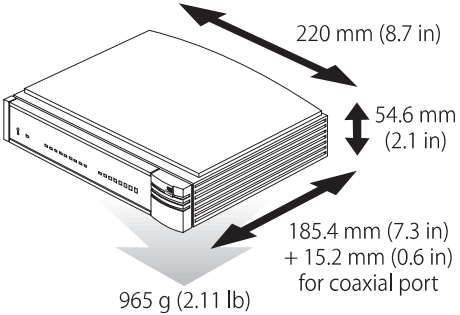
If necessary, consult your dealer, service representative, or an experienced radio/television technician for additional suggestions.

The manufacturer is not responsible for any radio or television interference caused by unauthorized modifications to the product. It is the responsibility of the user to correct such interference.

You must use shielded interface cables and a ferrite in order to maintain compliance with the limits for a Class B device.

CAUTION: *Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the product.*

Dimensions



18 VA
61 BThU/hr
power requirement

0-40°C (32-105°F)
operating
temperature

0-90%
(non-condensing)
humidity

Interface Cable Characteristics

WAN Port Connecting Cable – V.11/X.21 Support

The WAN port terminates with a 25-way D-type female connector. The port can be configured to support V.11 signalling characteristics at data transfer rates up to 2.048 Mbps. The WAN port connecting cable is not supplied with the unit. The following signalling characteristics should be observed when purchasing or fabricating a suitable cable.

Pin Links	3Com end pin no. (25-way male)	Signal name	Client end pin no. (15-way male D-type connector)
	2	Transmit Data A (TXDA)	2
	3	Receive Data (RXDA)	4
	7	Signal Ground (Receive Data)	8
	12	Signal Ground	
	13	Indicate B (INDB)	12
	14	Transmit Data B (TXDB)	9
	15	Indicate A (INDA)	5
	16	Receive Data B (RXDB)	11
	17	Clock A (CLKA)	6
	19	Clock B (CLKB)	13
	23	Control B (CTRLB)	10
	24	Control A (CTRLA)	3

WAN Port Connecting Cable – V.24/V.28 Support

The WAN port terminates with a 25-way D-type female connector. The port can be configured to support V.24 or V.28 signalling characteristics at data transfer rates up to 19.2 Kbps. The WAN port connecting cable is not supplied with the unit. The following signalling characteristics should be observed when purchasing or fabricating a suitable cable.

Pin Links	3Com end pin no. (25-way male D-type connector)	Signal name	Client end pin no. (25-way male D-type connector)
	2	Transmit Data (TXD 103)	2
	3	Receive Data (RXD 104)	3
	4	Request To Send (RTS 105)	4
	5	Clear To Send (RTS 106)	5
	6	Data Set Ready (DSR 107)	6
	7	Signal Ground (102)	7
	8	Data Carrier Detect (DCD 109)	8
	11	Signal Ground (AutoSense)	
	12	Signal Ground (AutoSense)	
	15	Transmit Clock (TXCLK 114)	15
	17	Receive Clock (RXCLK 115)	17
	18	Analog Loop Test (141)	18
	20	Data Terminal Ready (DTR 108)	20
	21	Remote Digital Loop Test (140)	21
	22	Ring Indicator (RI 125)	22
	24	External Clock (EXCLK) If clock signals are required, connect Pin 24 to Pins 15 & 17 at the 3Com end only.	

WAN Port Connecting Cable – V.35/V.36 Support

The WAN port terminates with a 25-way D-type female connector. The port can be configured to support V.36 signalling characteristics at data transfer rates up to 48 Kbps. The WAN port connecting cable is not supplied with the unit. The following signalling characteristics should be observed when purchasing or fabricating a suitable cable.

Pin Links	3Com end pin no. (25-way male)	Signal name	Client end pin no. (34-way MRAC connector)
	2	Transmit Data (TXD 103)	P
	3	Receive Data (RXD 104)	R
	4	Request To Send (RTS 105)	C
	5	Clear To Send (RTS 106)	D
	6	Data Set Ready (DSR 107)	E
	7	Signal Ground (102)(Clear To Send)	B
	8	Data Carrier Detect (DCD 109)	F
	11	Signal Ground	
	13	Serial Clock Transmit B (SCTB 114)	AA
	14	Transmit Data B (TXDB 103)	S
	15	Serial Clock Transmit A (SCTA 114)	Y
	16	Receive Data B (RXDB 104)	T
	17	Serial Clock Receive A (SCRA 115)	V
	19	Serial Clock Receive B (SCRB 115)	X
	20	Data Terminal Ready (DTR 108)	H

Manager Port Connecting Cable

The manager port cable terminates with a 9 pin female connector at one end and a 9-pin male/female D-type connector or 25-pin D-type male/female connector. The pin-out tables below show the pin outs for both variants.

3Com end pin no. (9-way male connector)	**Signal Name**	**Pin Links**	**Signal Name**	**Terminal or Com port end pin number** (9-way male/female connector)
Shell	Screen		Screen	Shell
3	TxD		RxD	2
2	RxD		TxD	3
5	Ground		Ground	5
7	RTS (not connected)		RTS (not connected)	7
8	CTS		DTR	4
6	DSR		CTS	8
1	DCD		DSR	6
4	DTR		DCD	1

3Com end pin no. (9-way male connector)	**Signal Name**	**Pin Links**	**Signal Name**	**Terminal or Com port end pin number** (25-way male/female connector)
Shell	Screen		Screen	1
3	TxD		RxD	3
2	RxD		TxD	2
5	Ground		Ground	7
7	RTS (not connected)		RTS (not connected)	4
8	CTS		DTR	20
6	DSR		CTS	5
1	DCD		DSR	6
4	DTR		DCD	8

Modem Cable

If you want to connect to the manager port using a modem, you will need a cable as shown in the table below. This connects the manager port's 9 pin D-type connector to a 25-pin serial port on a modem.

3Com end pin no. (9-way male connector)	**Signal Name**	**Pin Links**	**Signal Name**	**Terminal or Com port end pin number** (25-way male/female connector)
Shell	Screen		Screen	1
3	TxD		TxD	2
2	RxD		RxD	3
7	RTS		RTS	4
8	CTS		CTS	5
6	DSR		DSR	6
5	Ground		Ground	7
1	DCD		DCD	8
4	DTR		DTR	20

LAN Port Connecting Cable - 10BaseT

The 10BaseT port terminates with an RJ45 connector which can be connected to the 10BaseT port on another device. The table below shows the pin-outs for a straight through cable.

Pin Links	**3Com end pin no.** (RJ45)	**Signal name**	**Client end pin no.** (RJ45)
	1	TxD+	1
	2	TxD-	2
	3	RxD+	3
	4	not used	4
	5	not used	5
	6	RxD-	6
	7	not used	9
	8	not used	10

Ordering Information

3C410000 OfficeConnect Remote 510s
3C410005 OfficeConnect Remote 520s
3C4100010 OfficeConnect Remote 530s
3C4100015 OfficeConnect Remote 510u
3C4100020 OfficeConnect Remote 520u
3C4100025 OfficeConnect Remote 530u

3C16740 Power adapter (US)
3C16741 Power adapter (UK)
3C16742 Power adapter (Mainland Europe)
3C16743 Power adapter (Japan)
3C16744 Power adapter (Australasia)
3C16745 Power Adapter (South Africa)

731/000036 9-pin D-type plug to 9-pin D-type socket, gender changer (Serial Management port cable).

731/000024 9-pin D-type plug to RJ45 plug, with 3 meters of cable.

733/000028 RJ45 to RJ45 plug, with 1.5 meters of UTP cable (ISDN cable).

733/000001 RJ45 to RJ45 plug, with 3 meters of UTP cable (ISDN cable).

3C409000 25-pin to 25-pin D-type plug, with 3 meters of cable (V.24).

3C409001 25-pin D-type plug to 34-way MRAC connector, with 3 meters of cable (V.35).

3C409004 25-pin to 15-pin D-type plug, with 3 meters of cable (X.21).

733/000026 British Telecom socket to RJ11 converter (UK only).

980/000033 OfficeConnect Remote User Guide.

C GLOSSARY

10Base2 An IEEE standard for using IEEE 802.3 protocol at 10 Mbps over thin Ethernet cable.

10Base5 An IEEE standard for using IEEE 802.3 protocol at 10 Mbps over thick Ethernet cable.

10BaseT An IEEE standard for using IEEE 802.3 protocol at 10 Mbps over unshielded twisted-pair cable (the *T* stands for twisted pair).

100BaseVG An IEEE standard for using the new IEEE 802.12 protocol at 100 Mbps over unshielded twisted-pair cable of type 5 or type 3.

100BaseT A proprietary standard for using IEEE 802.3 protocol at 100 Mbps over unshielded twisted-pair cable. IEEE standards approval pending.

802.3 An IEEE standard for the physical layer that specifies a CSMA/CD protocol. This is the standard protocol used for Ethernet. Refer to *CSMA/CD*.

Address The unique code assigned to each device or workstation connected to the LAN.

Age The process of removing an address from the unit's filtering database after the device has not transmitted for a given period of time.

ANSI American National Standards Institute.

Application layer Layer seven, the uppermost part of the OSI network layer model. This layer contains the user and application programs.

ASCII American Standard Code for Information Interchange, a standard that defines the values that are used for letters, numbers, and symbols.

Attenuation The progressive degradation of a signal as it travels through a cable.

AUI Attachment user interface, the interface between the unit and the data terminal equipment, usually in the form of a connecting cable.

B Channel A digital data communications channel running at 64 Kbps. The basic rate ISDN 2 service carries two B channels plus one control D channel. Refer to *ISDN* and *D Channel*.

Backbone A network cabling segment that interconnects a group of network segments or systems.

Bandwidth The capacity of data communications system or channel.

Baseband A communication technique in which network cable is used to carry a single stream of data at a time.

Baud A unit of signalling speed equal to the number of signalling events in one second.

Bit Either of the digits 0 or 1 when used in the binary numeration system. Eight bits equals a single byte.

Bridge A device that links two or more local or remote area networks together. A bridge may be used to extend the network or to connect two different network transport technologies together.

Broadband A communications technique in which network cabling is used to carry multiple streams of data simultaneously.

Broadcast Storm A rare event in which broadcast frames are propagated endlessly through the network because poorly configured bridge and router connections.

Bus A single segment through which devices are connected. An Ethernet LAN is based on a bus network which connects all communicating workstations with a common cable.

Byte A string that consists of eight data bits treated as a unit.

Call Guillotine A feature that disconnects a call after a certain period of time irrespective of whether data is being passed across the link or not.

CCITT Comité Consultatif International Téléphonique et Télégraphique, now renamed ITU, International Telecommunication Union.

CHAP Challenge Handshake Authentication Protocol. Part of the PPP protocol to ensure authentication of the connection between two devices.

Class Type of IP address. IP addresses fall into three main classes, A, B and C.

Client A user whom is making use of a particular system resource or peripheral through a workstation attached to a local or wide area network.

Client/server A user who is attached to a file server to recover and store files, but the processing of the data or use of an application is carried out on the client machine.

Coaxial cable A twin-conductor cable used for computer networking, in either a thick or thin form. This cable consists of a centre core wire (stranded or single core) covered by insulation, a second conductor of woven wire, and an external covering of rubber. Thin coaxial cable resembles television cable. Thick coaxial cable has an increased diameter outer bore and is often yellow or orange in color.

CSMA/CD Carrier Sense Multiple Access with Collision Detection, the Ethernet protocol that allows each device to create and send its own data packets. CSMA/CD is used to avoid excessive collisions between packets as they are randomly transmitted. A CSMA/CD device first listens for other carriers, if it detects no other carriers, it will then allow the data packet to be transmitted. If a collision is detected, the device stops transmitting, waits a random length of time, and begins transmitting again.

D Channel A control channel carrying signalling information, running at 16 Kbps. The basic rate ISDN 2 service carries two B channels plus one control D channel. Refer to *ISDN* and *B Channel*.

Data Characters or code either entered by the user or passed between devices that are part of the computer or network.

Data communications The transfer of data via transceiver equipment by means of data transmission according to a protocol. Refer to *Protocol*.

Datagram A message that is sent from one computer or device to another to confirm it location or status on a network.

Data link layer The second layer of the OSI reference model. This layer is responsible for controlling message traffic.

Data packet (packet) A sequence of binary digits, including data and control signals that is transmitted across a LAN or WAN.

DCE Data circuit-terminating equipment.

DTE Data Terminal Equipment. The physical interface and link access procedures between DTE and data circuit-terminating equipment (DCE).

DTMF Dial tone multi-frequency, the signalling system used by PSTN. Refer to *PSTN*.

Downloading A user initiated transfer of data from a server to the user's own workstation. Also used to classify the transfer of files from one system to another, usually to upgrade or revise system software.

EPROM Erasable programmable read-only memory. A chip whose memory can be erased and reused.

Ethernet A 10 Mbps baseband local area network protocol, compatible with IEEE 802.3 standards.

FastConnect The OfficeConnect Remote's proprietary connection protocol that allows fast connection between units either over the ISDN link or over a permanent leased line WAN link.

Fiber optics A technology that uses laser light pulses, sent over thin glass fibres, which is able to deliver data at speed up to several gigabits per second.

File server A computer running a special operating system that allows workstations to access files.

Filter A configuration that removes types of data frames based on user-entered parameters.

Firewall A method of preventing unauthorized access to a network or a host on a network. A firewall is usually implemented within a router's software.

Frame The method by which a data packet is constructed to be sent across a network. Usually assembled with header and footer information.

Gateway Another name for a router on a network.

HDLC High-level Data Link Control. OSI's bit orientated protocol.

Hop count The number of routing nodes between a source and destination device on a LAN or WAN.

Host A device or computer on an IP network to which you can connect.

Hub A cabling centre in a star topology that either amplifies a signal and transmits it (active hub) or simply passes the signal along (passive hub).

Hyperterminal The terminal emulation program provided with Microsoft Windows 95™.

IEEE The Institute of Electronic and Electrical Engineers.

IPX Internetwork Packet Exchange, the default data packet protocol for Novell's NetWare operating system.

ISDN Integrated Services Digital Network. A multi-channel digital end-to-end telecommunications network that provides a virtually error free transmission of data.

ISO International Standards Organization. Refer to *Open Systems Interconnection*.

Kbps A measurement of data transmission speed in kilo bits per second.

Keep alives A message sent by one network device to inform another network device that the virtual circuit between them is still active.

LAN Local area network, a network that covers a group of local workstations and peripherals that require to share information.

Learn A bridge learns addresses received at any of its interfaces and adds them to its filter address table.

MAC Medium access control, a protocol for determining which device has access to the network at any one time.

Mbps A measurement of data transmission speed in megabits per second.

MAN Metropolitan area network, a network that covers a city.

MIB Management information base.

NETBIOS Network Basic Input/Output System, a standard for supporting network communications that is independent of the underlying network transport type.

NetWare Novell's Network Operating System (NOS) line.

Network A method of connecting computers and other devices together with cabling so that they can communicate with each other.

NIC Network interface card, an expansion card that enables a PC to communicate on a network.

Network layer The third layer of the OSI reference model. This layer is responsible for controlling message traffic.

NFS A network file system developed by Sun Microsystems for shared files over a UNIX platform.

Node An alternative name for a computer or device (such as a printer or modem) that is connected to a network.

NOS Network operating system.

OSI Open Systems Interconnection, a body of standards set by the International Standards Organization to define the activities that must occur when computers communicate. There are seven layers, and each contains a specific set of rules to follow at that point in the communication.

PAP Password Authentication Protocol. Part of the PPP protocol to ensure authentication of the connection between two devices.

Peer-to-peer network A network which contains workstations which are able to act as both client and client servers.

Piggyback A way of transmitting routing information over ISDN lines by adding it to valid data frames. This avoids ISDN calls being generated solely for passing routing information.

Physical layer The first layer of the OSI network layer model. This layer manages the transfer of individual bits of data over wires, or whatever medium, that is used to connect workstations and peripherals.

Polling A method of controlling terminals on a multi-point network where each device is interrogated, in turn, to determine if the device is ready to receive or transmit data.

PPP Point-to-Point Protocol. The de facto standard protocol for routing between devices made by different manufacturers.

Presentation layer The sixth layer of the OSI network layer model. This layer controls the formatting and translation of data.

Protocol A set of rules and procedures that govern the exchange of data between two communicating systems.

PSTN Public switched telephone network.

Quick Configuration A set of menu driven forms in the management system that allow you to configure the unit for most types of ISDN connection.

REN Ringer equivalence number.

RIP Routing information protocol.

Router A protocol transparent device that links networks. A router can be used to separate unwanted traffic on either side of the bridge, reduce the traffic, or to provide security from unauthorized users.

SAP Source address protocol.

Segment A section of an Ethernet network, typically connected by repeater or a bridge to another segment.

SPX Sequenced Packet Exchange, Novell's guaranteed-delivery version of IPX.

Session A logical connection between two communicating systems that allows for the transfer of data.

Session layer The fifth layer of the OSI network layer model. This layer is responsible for the security and administrative tasks of communicating.

SNMP Simple network management protocol, a software program to allow the remote management of bridge and routing devices.

Static Route A route you have entered and made permanent rather than a route that the unit has learned by connecting to other routers.

STP Spanning tree protocol, a protocol which prevents network loops.

Terminal The Microsoft Windows™ terminal emulation program.

Terminators Devices that are used at the ends of a linear bus network segment to reflect the signal back and prevent failure of the segment.

TCP/IP Transmission control protocol/Internet protocol, a set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

Thick Ethernet A cabling system for Ethernet connections that uses a heavyweight coaxial cable. Suitable for large networks.

Thin Ethernet A cabling system for Ethernet connections that uses a lightweight coaxial cable. Suitable for small networks.

Ticks A measurement of the time taken to pass information through a routed network.

Token Ring A network transport technology in which an electronic token that allows access to the network is passed around stations in the ring.

Topology The way that a network is physically laid out.

Transport layer The fourth layer of the OSI network layer model. This is responsible for error checking and correction, and some message flow control.

WAN Wide area network, a network that covers a wide area and requires special communication devices (bridges and/or routers) to make connection possible. WANs make connections over long distances and need telephone, satellite, or microwave equipment to allow connections to be made.

Workstation Another name for a computer or device (such as a printer or modem) that is connected to a network.

D TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

On-line Technical Services

3Com offers worldwide product support seven days a week, 24 hours a day, through the following on-line systems:

- 3Com Bulletin Board Service (3ComBBS)
- World Wide Web site

3Com Bulletin Board Service

3ComBBS contains patches, software, and drivers for all 3Com products, as well as technical articles. This service is available via modem or ISDN seven days a week, 24 hours a day.

Access by Modem To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	Data Rate	Telephone Number
Australia	up to 14400 bps	(61) (2) 9955 2073
France	up to 14400 bps	(33) (1) 69 86 69 54
Germany	up to 9600 bps up to 9600 bps	(49) (89) 627 32 188 (49) (89) 627 32 189
Hong Kong	up to 14400 bps	(852) 2537 5601
Italy (fee required)	up to 9600 bps	(39) (2) 273 00680
Japan	up to 14400 bps	(81) (3) 3345 7266
Singapore	up to 14400 bps	(65) 534 5693
Taiwan	up to 14400 bps	(886) (2) 377 5838
U.K.	up to 14400 bps	(44) (1442) 278278
U.S.	up to 14400 bps	(1) (408) 980 8204

Access by ISDN ISDN users can dial-in to 3ComBBS using a digital modem for fast access up to 56kbps. To access 3ComBBS using ISDN, dial the following number: **(1) (408) 654 2703**

World Wide Web Site

Access the latest networking information on 3Com's World Wide Web site by entering our URL into your Internet browser:

`http://www.3com.com/`

This service features news and information about 3Com products, customer service and support, 3Com's latest news releases, selected articles from 3TECH™ (3Com's award-winning technical journal) and more.

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Diagnostic error messages.
- A list of system hardware and software, including revision levels.
- Details about recent configuration changes, if applicable.

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to receive support from your network supplier, technical support contracts are available from 3Com.

In the U.S. and Canada, call **(800) 876-3266** for customer service.

If you are outside the U.S. and Canada, contact your local 3Com sales office to find your authorized service provider:

Country	Telephone Number
Australia (Sydney)	(61) (2) 959 3020
(Melbourne)	(61) (3) 653 9515

Country	Telephone Number
Belgium*	0800 71429
Brazil	(55) (11) 546 0869
Canada	(905) 882 9964
Denmark*	800 17309
Finland*	0800 113153
France*	05 91 79 59
Germany*	0130 821502
Hong Kong	(852) 868 9111
Ireland*	1 800 553117
Italy*	1678 79489
Japan	(81) (3) 3345 7251
Mexico	(525) 531 0591
Netherlands*	06 0227788
Norway*	80013376
Singapore	(65) 538 9368
South Africa	(27) (11) 803 7404
Spain*	900 983125
Sweden*	120 795482
Taiwan	(886) (2) 577 4352
United Arab Emirates	(971) (4) 349049
U.K.*	0800 966197
U.S.	(1) (408) 492 1790

* These numbers are toll free

Returning Products for Repair

A product sent directly to 3Com for repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to 3Com without an RMA number will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Country	Telephone Number	Fax Number
U.S. and Canada	(800) 876 3266, option 2	(408) 764 7120
Europe	31 30 60 29900 (option 5)	(44) (1442) 275822
Outside Europe, U.S. and Canada	(1) (408) 492 1790	(1) (408) 764 7290

INDEX

Numerics

10Base2 1-9
  connections 1-14
10BaseT
  connections 1-13
  crossover 1-9
  port 1-9
3Com Bulletin Board Service
  (3ComBBS) D-1
3Com sales offices D-2

A

ALERT LED 1-6

B

bridging and routing concepts A-1
bulletin board service D-1

C

clipping hubs together 1-11
clips 1-11
coaxial cable 1-9
commands
  IN 1-25
  IPB 1-22
  IPR 1-23
  NA 1-20
  NO 1-21
  QC 1-18
concepts - bridging and routing A-1
configuring your unit 1-17
connecting
  to a PC 1-9
connecting telephony equipment 1-16
connecting to 1-25
  Internet 1-25
  IP hosts on different networks 1-23
  IP hosts on same network 1-22
  Novell networks 1-21
  WAN leased line link 1-28
contents checklist 1-4
crossover switch 1-9

D

default password 1-18

E

Ethernet
  10Base2 port 1-14
  10BaseT port 1-9, 1-13
example networks 1-30

F

feet 1-11
front panel LEDs 1-6

H

hub
  clipping 1-11

I

installation 1-10
  10Base2 connections 1-14
  10BaseT connections 1-13
  ISDN connection 1-15
  management terminal connection 1-16
  power adapter 1-12
  pre-requisites 1-5
  siting the unit 1-10
  voice port connection 1-16
  wall mounting 1-12
ISDN
  connection 1-5, 1-9, 1-15
  port 1-9
ISDN OK LED 1-7
ISDN1 LED 1-7
ISDN2 LED 1-7

L

LAN
- 10Base2 connections 1-14
- 10BaseT connections 1-13
- 10BaseT port 1-9

LEDs
- Alert 1-6
- ISDN OK 1-7
- ISDN1 1-7
- ISDN2 1-7
- LINK STATE 1-7
- Network Utilization 1-7
- POWER 1-6
- SERIAL WAN 1-7
- VOICE 1-7

LINK STATE LED 1-7

M

management
- configuring your unit 1-17
- port 1-8

MDI/MDIX switch 1-9

N

network supplier support D-2
Network Utilization LEDs 1-7

O

on-line technical services D-1

P

package contents 1-4
password 1-18
power adapter 1-12
power inlet 1-8
POWER LED 1-6
PPP routers 1-25
problem solving 1-36

Q

Quick Configuration 1-17

R

rear panel
- 10BaseT port 1-9
- ISDN port 1-9
- power socket 1-8
- reset button 1-8
- serial port 1-8
- voice port 1-10
- WAN port 1-9

rear panel connections 1-8
registration card 1-5
reset button 1-8
returning products for repair D-3
rubber feet 1-11

S

serial port 1-8
SERIAL WAN LED 1-7
setting up your unit 1-17
siting the unit 1-10
stacking clips 1-11

T

technical support 1-5
troubleshooting 1-36

U

unit name 1-20

V

VOICE LED 1-7
voice port 1-10
VT100
- terminal connection 1-16

W

wall mounting 1-12
WAN
- connection 1-9
- port 1-9

WAN configuration 1-28

LIMITED WARRANTY

HARDWARE: 3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its Authorized Reseller:

Internetworking products	One year
Network adapters	Lifetime
Ethernet stackable hubs and Unmanaged Ethernet fixed port repeaters	Lifetime* (One year if not registered)
*Power supply and fans in these stackable hubs and unmanaged repeaters	One year
Other hardware products	One year
Spare parts and spares kits	90 days

If a product does not operate as warranted during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com pursuant to any warranty.

SOFTWARE: 3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its Authorized Reseller. 3Com warrants the magnetic media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation hereunder shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to 3Com's applicable published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty that its software products will work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a “bug” or defect in the third party's product.

STANDARD WARRANTY SERVICE: Standard warranty service for hardware products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to 3Com's Corporate Service Center or to an Authorized 3Com Service Center during the applicable warranty period. Standard warranty service for software products may be obtained by telephoning 3Com's Corporate Service Center or an Authorized 3Com Service Center, within the warranty period. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt by 3Com.

WARRANTIES EXCLUSIVE: IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

OFFICECONNECT REMOTE SUPPLEMENTARY INFORMATION

OfficeConnect Remote 531

The OfficeConnect Remote 531 provides the same functionality as the OfficeConnect 530, with the additional on-board memory allowing more sophisticated software (such as that provided by the OfficeConnect Remote /A software upgrade) to be installed in the unit.

Follow the OfficeConnect Remote 530 installation instructions described in the *OfficeConnect Remote User Guide*. Refer to the *OfficeConnect Remote Software Reference* if further configuration information is required.

EMC Update

The statement on page 4 of the *About This Guide* section in the *OfficeConnect Remote User Guide*, stating that the ISDN cable must be used in conjunction with a three turn ferrite to meet Class B of EN 55022, no longer applies.

© 3Com Europe Limited, December 1996
Part Number: 981-000077/001